(** \\ الحماية الشامله للأجهزة و البريد //**)

تأليف واعداد

انذار القناص :سنايبر أليرت



****

السلام عليكم ورحمة الله وبركاته

الحمد الله والصلاة والسلام على اشرف الانبياء و المرسلين سيدنا محمد وعليه افظل الصلاة واتم التسليم اما بعد :

اعددت هذا الكتاب نظرا لما رأيته في هذه الشبكة العنكبوتيه المليئه بالمشاكل ، من قرصنة و ملفات ضاره تجعل الجهاز مثل الشارع ليدخلوه الهكرز او مثل الفيروسات التي

تضر الجهاز وكثرة الشكاوي بالسرقة الايميلات واختراق الاجهزة :

هذا الكتاب اعددته ضد الهكرز الاطفال الذين يحاولون ويخططون في اختراق جهاز او ايميل شخص لا يعلم ما هو الهكرز وما هي الحمايه وهل جهازه محمي عند دخوله

للإنترنت لذلك صممت هذا الكتاب لتعرف كيف تحمي جهازك و ايميلك من السرقة وعدم تعرض جهازك لمخاطر الفايروسات

سأكتب لمحات بسيطه عن الحمايه اقبل ان ابدأ :

هل فكرت بيوم ان جهازك يخترق من قبل طفل هكر \ ويقوم بحذف ملفاتك وسرقة ايميلك ؟

هل فكرت بان طفل هكرز اخترق جهازك وقام بتصويرك ؟

هل فكرت بيوم ان جهازك مخترق من سنين وانت لا تعلم ؟

هل فكرت بان شخص يتجسس عليك وانت داخل الشبكة العنكبوتيه ؟

اذا انت جاهل ما دمت لا تعرف هذه الاشياء واعذرني على كلمة جاهل \ تخيل جهازك مخترق وشخص ما يتجسس عليك وانت لا تعلم او لديك كاميرا وقام بتصويرك وانت لا تعلم

او قام بسرقة بريديك او اطلع على الرسائل او يتجسس ما تفعله وما تكتبه

اذا تعلم من الان كيف تحمي نفسك لانه لا يوجد احد قادر على حمايتك او من يساعدك في الحمايه فتعلم قبل فوات الاوان

ايضا هناك فايروسات خطيره جدا والبعض يقول جهازي لا يوجد به فايروس لان جهاز ليس عطلان فتذكر ان اخبث الفايروسات تدمج نفسها في ملفات تنفيذية او ملفات انترنت

او ملفات com و dll وعند قيامك بفحص الجهاز من الفايروسات تجد اغلب البرامج المهمه لديك مدموجه بفايروس وعند حذف الفايروس يحذف ملف البرنامج معه

فلماذا لم تقم بحماية نفسك في البدايه قبل دخول هذا الفايروس .. اذا هذا الكتاب بإذن الله سيفيدك في الحمايه

على بركة الله نبدأ

بداية لك قم بعمل فورمات للجهاز لتجنب الفايروسات القديمه التي بجهازك ثم قم بتنصيب برنامج الحمايه فورا بعد الفورمات واياك الدخول على الاقراص الاخرى بعد

الفورمات ايضا اياك الدخول على اي وصلة تخزين قابله للإزالة مثل الميموري فلاش او ذاكرة الجوال او سيدي طيب نحن كذا تمام

هناك انواع لبرامج الحماية والكل لا يعلم ما هو افظلها ! فمن ناحيتي ابدأ الان افظل برنامج يسمى بالافيرا ، هذا البرنامج ياعتبره من اقوى برامج الحماية

فإذا وضعته بجهازك فأعتبر انك اكملت نص المشوار – طيب من أين أجد هذ البرنامج ؟

لنفرض لم تقم بعمل فورمات تاااابع الصور

اولا : قم بحذف البرنامج الحمايه الذي لديك ان كان الكاسبر او النود32 ...إلخ وهذا شرح بالصور لكيفية حذف أي برنامج بجهازك !

اولا اذهب إلى : ابدأ + اعدادات + لوحة التحكم + اضافة وازالة البرامج !



جميل جدا \ طبعا لم اقم بحذفه لان يختلف البرنامج الذي لديك

طيب بعد حذفه قم بإعادة تشغيل الجهاز \ وبعدها اذهب إلى هذا الرابط لتحميل برنامج الحمايه المسمى بالافيرا

اذهب الى هذا الرابط لموقع البرنامج طبعا البرنامج تجريبي بامكانك شراء نسخه اصليه من اي محل كمبيوتر وقيمته85 ريال او 95 ريال

http://www.free-av.com/en/trialpay_download/1/avira_antivir_personal__free_antivirus.html

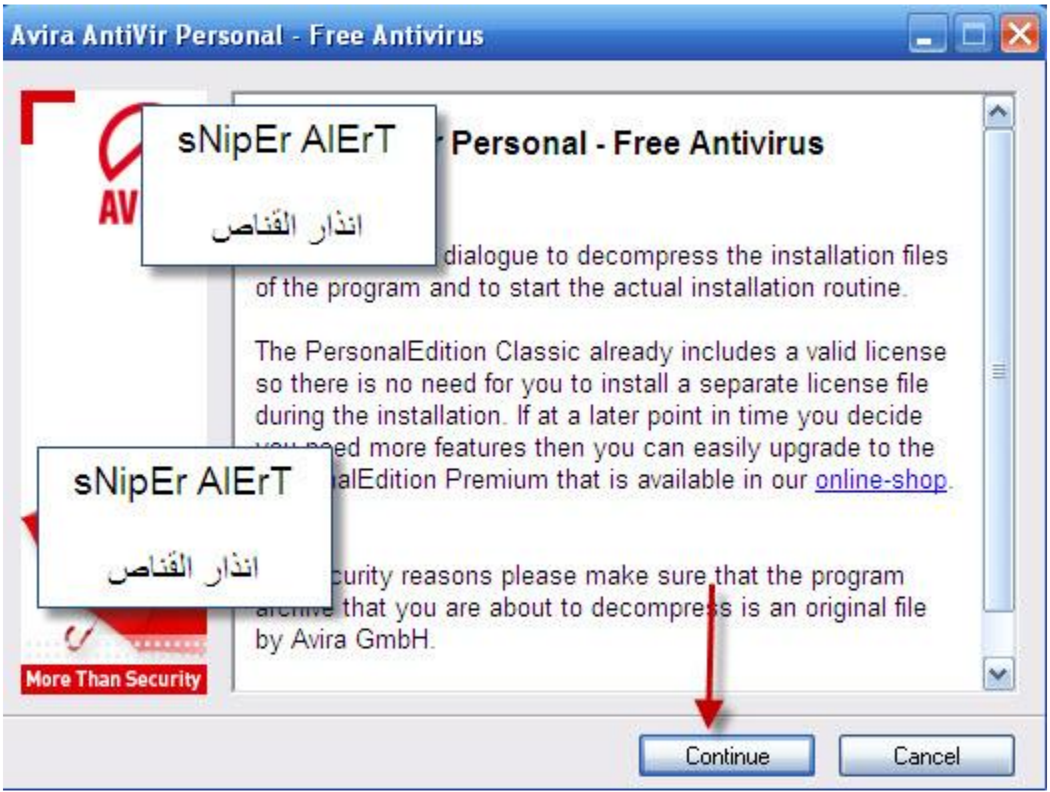

Search:
Google™ Custom Search
Go
Language:
English
اضغط هنا
OWNLOAD
SUPPORT
COMMUNITY
SHOP
ontinue to Download
AntiVir Free Version
sNipEr AlErT
انذار القناص
nium
REE
Recommended Download
DOWNLOAD NOW!
Download.com
Or...
Reg. £12.95
wnload Avira AntiVir Personal - FREE
us from the following locations:
oftpedia
Download.com

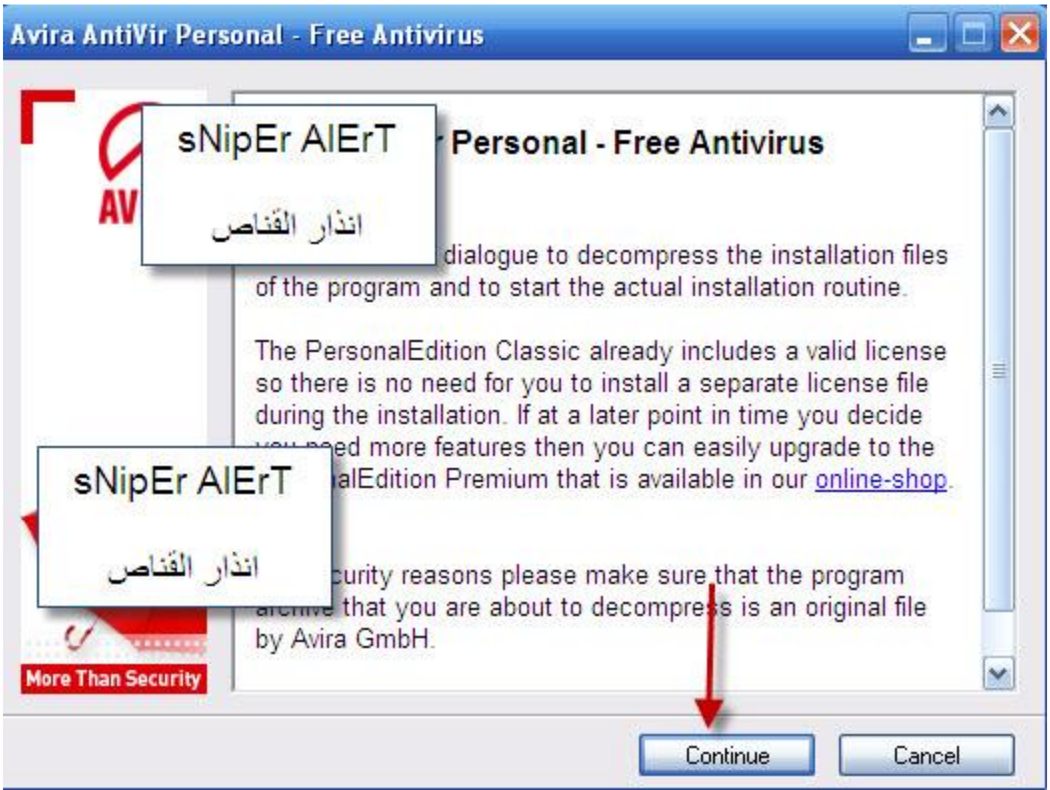

home | reviews | news
downloads
cnet tv
On ZDNet: Why I Will never buy a Mac
cnet download.com
sNipEr AlErT
انذار القناص
Windows
Mac
Mobile
Home » Windows Downloads » Security Software » Antivirus Software
Welcome
اضغط هنا
iVir Personal - Free Antivirus users
CNET Download.com is the safe and trusted provider for Avira AntiVir Personal - Free Antivirus 9.0.0.403
To complete your download, click on the link below:
Download Now (30.8MB)
Tested spyware free



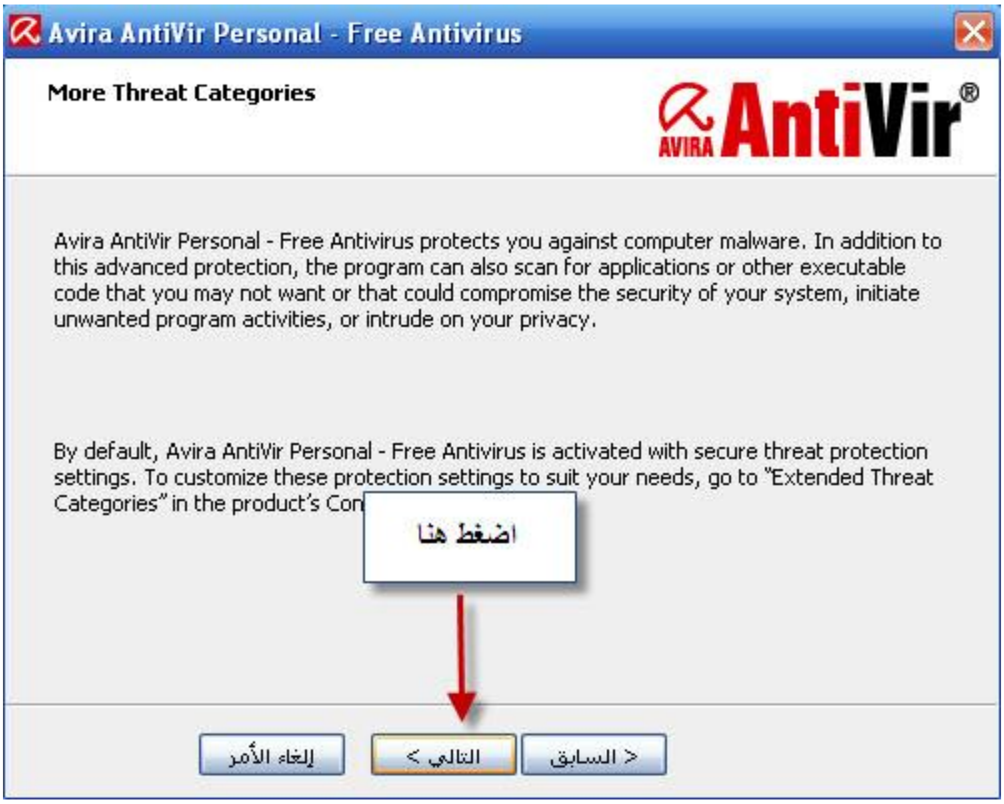


تابع معي عملية التنصيب :


Avira AntiVir Personal - Free Antivirus
sNipEr AlErT
انذار القناص
Personal - Free Antivirus
dialogue to decompress the installation files of the program and to start the actual installation routine.
The PersonalEdition Classic already includes a valid license so there is no need for you to install a separate license file during the installation. If at a later point in time you decide
ed more features then you can easily upgrade to the
alEdition Premium that is available in our online-shop.
sNipEr AlErT
انذار القناص
urity reasons please make sure that the program
that you are about to decompress is an original file by Avira GmbH.
More Than Security
Continue
Cancel


Avira AntiVir Personal - Free Antivirus
sNipEr AlErT
انذار القناص
Personal - Free Antivirus
dialogue to decompress the installation files of the program and to start the actual installation routine.
The PersonalEdition Classic already includes a valid license so there is no need for you to install a separate license file during the installation. If at a later point in time you decide
ed more features then you can easily upgrade to the
alEdition Premium that is available in our online-shop.
sNipEr AlErT
انذار القناص
urity reasons please make sure that the program
that you are about to decompress is an original file by Avira GmbH.
More Than Security
Continue
Cancel


Avira AntiVir Personal - Free Antivirus
sNipEr AlErT
انذار القناص
AVIRA
Welcome to the setup for
Avira AntiVir Personal
This wizard will install Avira AntiVir
your computer.
click Next.
اضغط هنا
إلغاء الأمر
التالي >


Avira AntiVir Personal - Free Antivirus
More Threat Categories
AVIRA AntiVir®
Avira AntiVir Personal - Free Antivirus protects you against computer malware. In addition to this advanced protection, the program can also scan for applications or other executable code that you may not want or that could compromise the security of your system, initiate unwanted program activities, or intrude on your privacy.
By default, Avira AntiVir Personal - Free Antivirus is activated with secure threat protection settings. To customize these protection settings to suit your needs, go to "Extended Threat Categories" in the product's Con
اضغط هنا
إلغاء الأمر
التالي >
< السابق

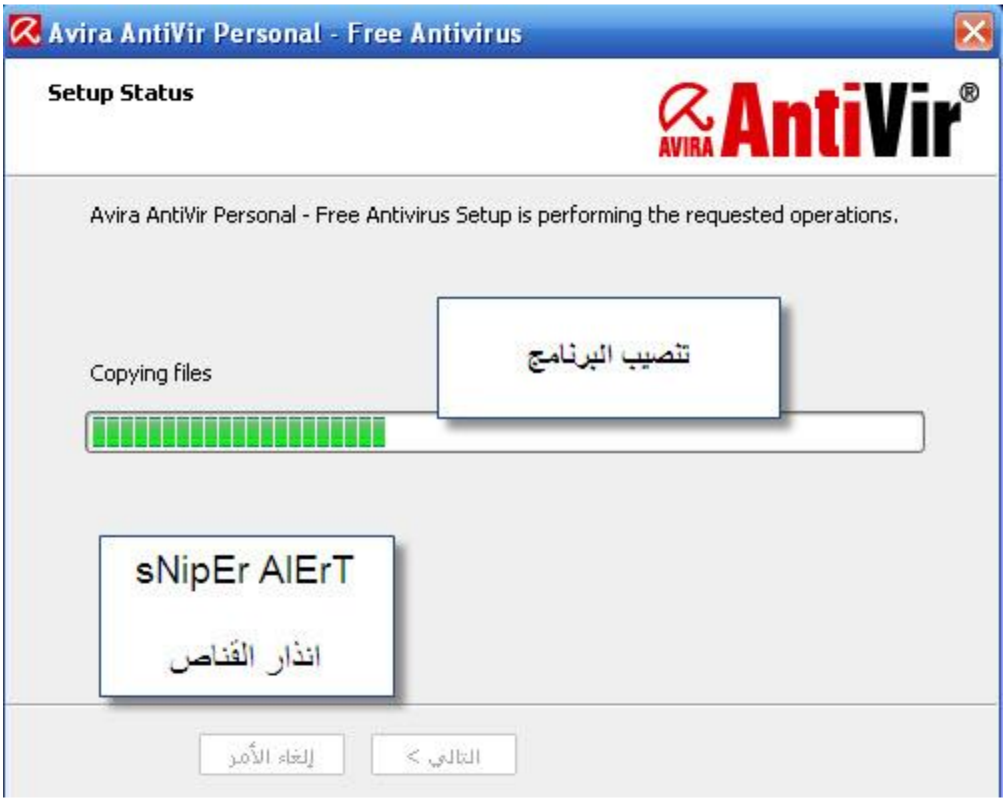

Avira AntiVir Personal - Free Antivirus
Accept Lice
sNipEr AlErT
انذار القناص
AntiVir
AVIRA
Licence agreement Avira AntiVir Personal - Free AntiVirus
Please read through the following software licence agreement. By installing the software, you explicitly agree to be bound by the conditions of this agreement. If you do not accept the conditions of this agreement, you may not use the software.
This free Avira AntiVir Personal - Free AntiVirus is intended exclusively for private use on a single workstation. You may copy the complete program package and pass it on to others for pr
ira AntiVir Personal - Free
AntiVirus may not be used
ional purposes.
اضغط هنا
I accept the terms of the license agreement
إلغاء الأمر
التالي <
السابق >


Avira AntiVir Personal - Free Antivirus
Confirmation
AntiVir
AVIRA
sNipEr AlErT
انذار القناص
Please confirm that you will use the Avira AntiVir Personal - Free Antivirus only for private and not for commercial purposes.
I accept that Avira AntiVir Personal - Free Antivirus is for private use only and must not be used for any kind of commercial or business purpose.
إلغاء الأمر
التالي <
السابق >


Avira AntiVir Personal - Free Antivirus
Choose Installation Type
sNipEr AlErT
انذار القناص
Please select a setup type.
Complete
All program features will be installed.
Custom
Select the program features you want to install. Recommended for advanced users.
إلغاء الأمر
التالي <
السابق >

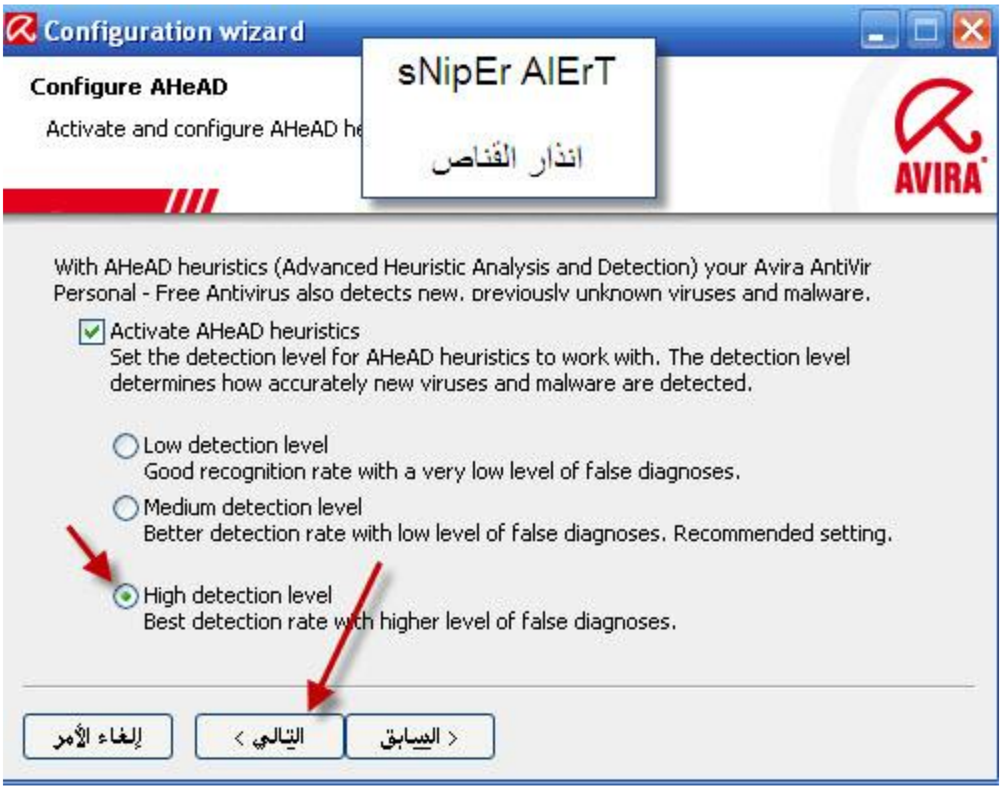

Avira AntiVir Personal - Free Antivirus license wizard
sNipEr AlErT
انذار القناص
Registration
ادخل بيانات من راسك
Please enter your personal details
Title:*
Mr
* = required fields
First name:*
Surname:*
Email:*
Repeat email:*
Street:
Postal code:
City:
Country:*
SAUDI ARABIA
Telephone:
Yes, I would like to subscribe to the Avira newsletter
Yes, I would like to register as a user of Avira AntiVir Personal - Free Antivirus
إلغاء الأمر
التالي <
السابق >

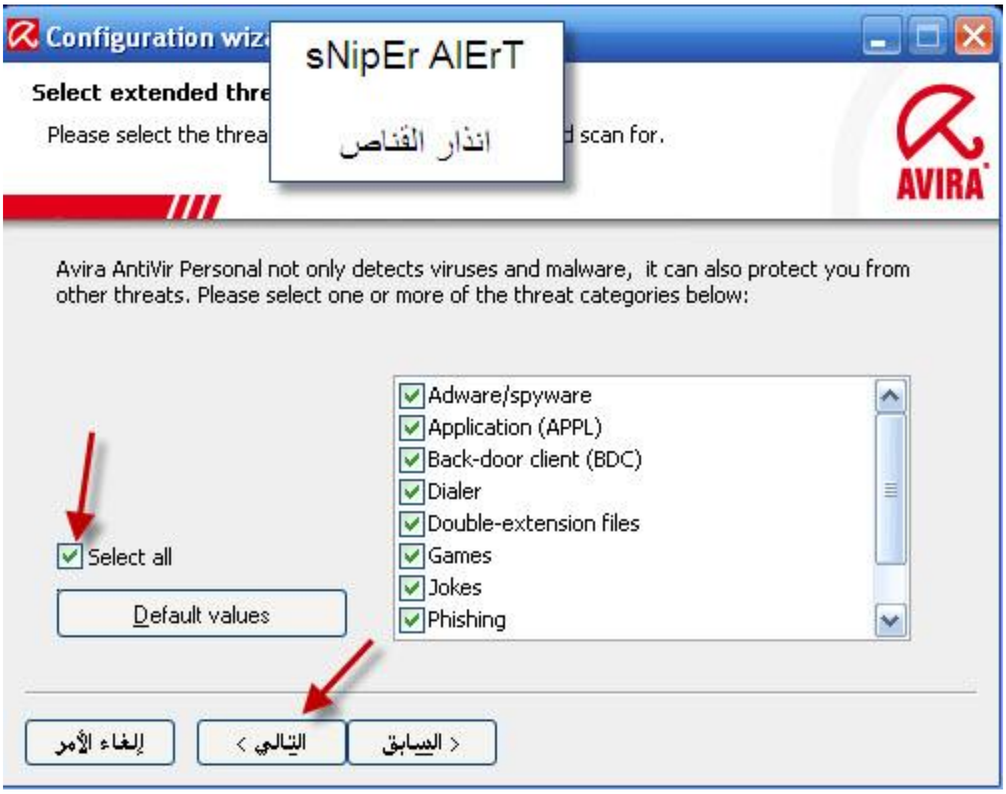

Avira AntiVir Personal - Free Antivirus license wizard
Result
sNipEr AlErT
انذار القناص
Your re
you.
Further information on your product can be found at www.free-av.com
اضغط هنا
إلغاء الأمر
التالي <
السابق >


Avira AntiVir Personal - Free Antivirus
Setup Status
Avira AntiVir Personal - Free Antivirus Setup is performing the requested operations.
Copying files
تنصيب البرنامج
sNipEr AlErT
انذار القناص
إلغاء الأمر
التالي <

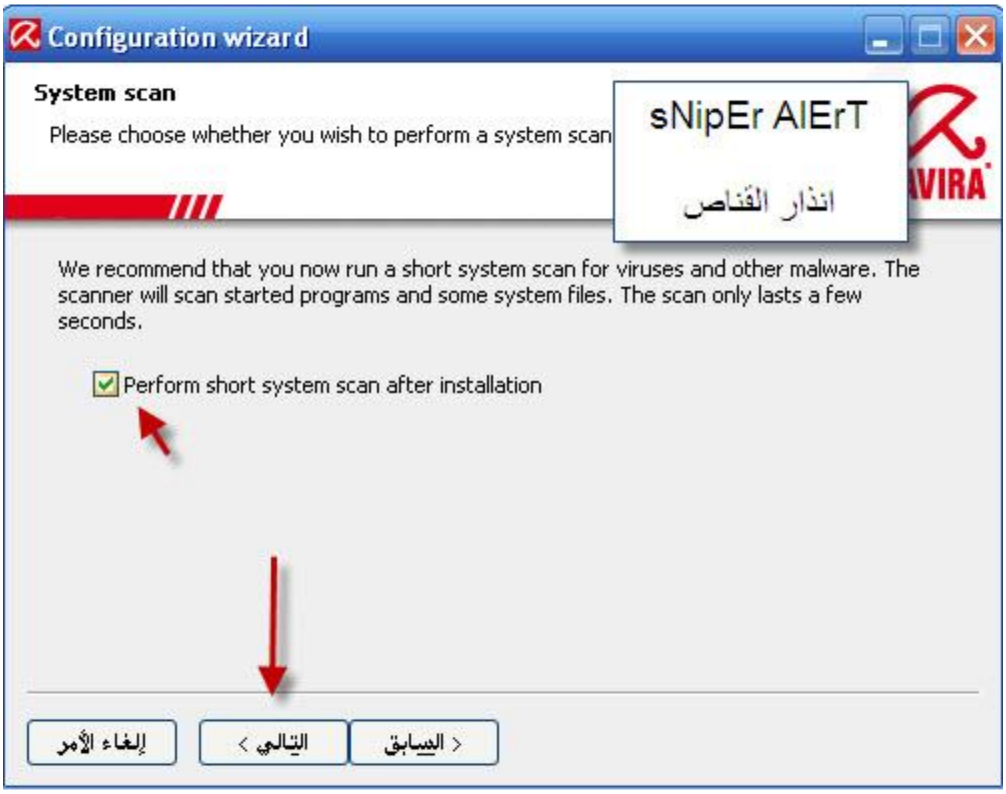

Avira AntiVir Personal - Free Antivirus
sNipEr AlErT
انذار القناص
AVIRA
Installation complete
The installation of Avira AntiVir Personal was successful.
Show readme.txt
Press Finish to end setup.
إلغاء الأمر
إنهاء


Configuration wizard
Welcome to the Configuration Wizard
sNipEr AlErT
انذار القناص
AVIRA
Please note that automatic updates are already pre-configured. You can modify the settings as required in the Scheduler.
إلغاء الأمر
التالي <
< السابق


Configuration wizard
sNipEr AlErT
انذار القناص
Configure AHeAD
Activate and configure AHeAD he
With AHeAD heuristics (Advanced Heuristic Analysis and Detection) your Avira AntiVir Personal - Free Antivirus also detects new, previously unknown viruses and malware.
Activate AHeAD heuristics
Set the detection level for AHeAD heuristics to work with. The detection level determines how accurately new viruses and malware are detected.
Low detection level
Good recognition rate with a very low level of false diagnoses.
Medium detection level
Better detection rate with low level of false diagnoses. Recommended setting.
High detection level
Best detection rate with higher level of false diagnoses.
إلغاء الأمر
التالي <
> السابق
AVIRA


Configuration wiz
sNipEr AlErT
انذار القناص
Select extended thre
Please select the threa
d scan for.
Avira AntiVir Personal not only detects viruses and malware, it can also protect you from other threats. Please select one or more of the threat categories below:
Adware/spyware
Application (APPL)
Back-door client (BDC)
Dialer
Double-extension files
Games
Jokes
Phishing
Select all
Default values
إلغاء الأمر
التالي <
> السابق
AVIRA


Configuration wizard
Guard start mode
Please select the required G
sNipEr AlErT
انذار القناص
AVIRA
Normal start
Recommended default setting where AntiVir Guard starts in normal automatic mode.
Secure start
AntiVir Guard starts as early as possible. This early start offers more security but extends the time until the computer is available.
إلغاء الأمر
التالي <
> السابق


Configuration wizard
System scan
Please choose whether you wish to perform a system scan
sNipEr AlErT
انذار القناص
AVIRA
We recommend that you now run a short system scan for viruses and other malware. The scanner will scan started programs and some system files. The scan only lasts a few seconds.
Perform short system scan after installation
إلغاء الأمر
التالي <
> السابق

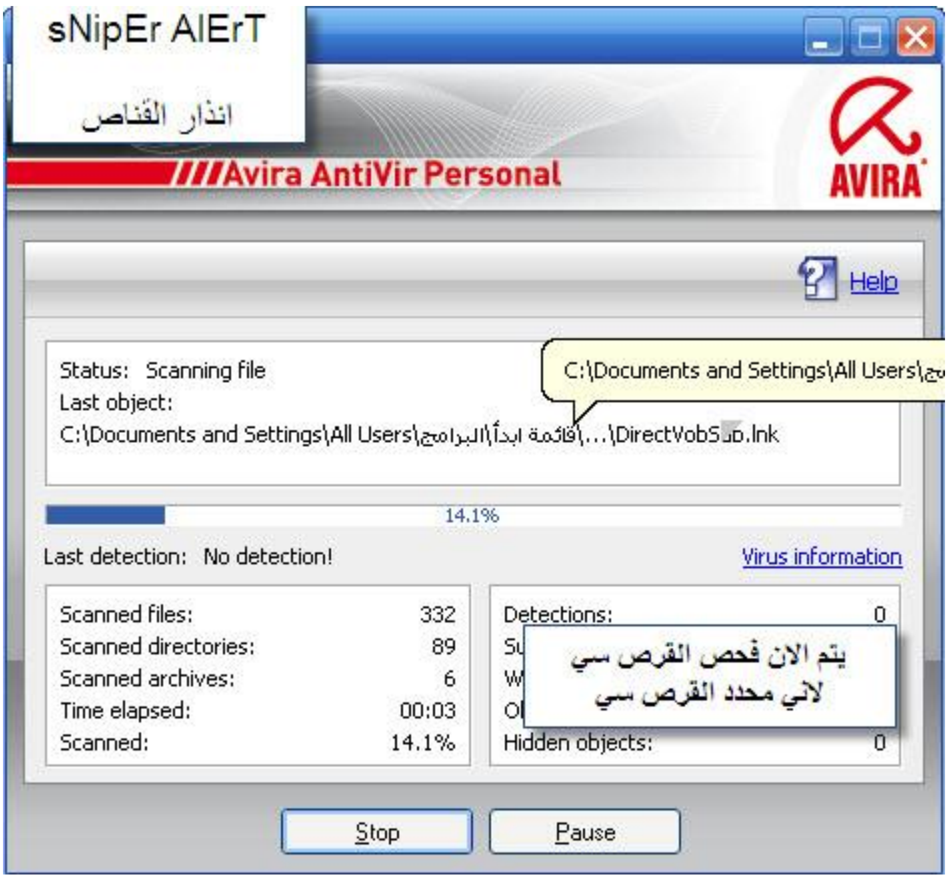


انتهينا من تنصيب برنامج الافيرا

عملية فحص الجهاز:



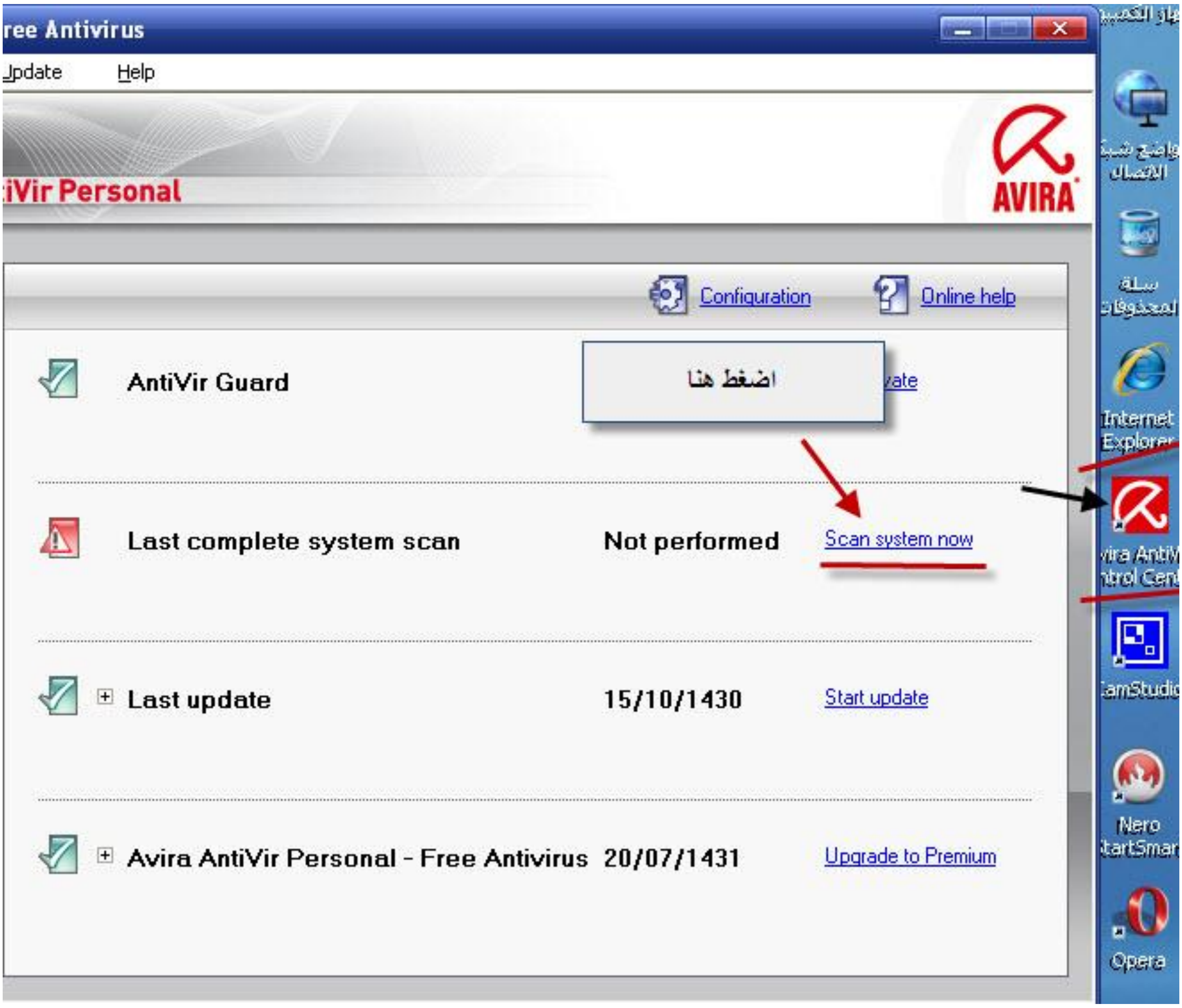
القرص المحلي (C:)
فتح
استكشاف
بحث...
مشاركة وأمان...
Scan with Trojan Remover
DVD-RAM (F:)
فحص C:\
Scan selected files with AntiVir
Add to archive...
"Add to "Archive.rar
Compress and email...
Compress to "Archive.rar" and email
Upload using WS_FTP Upload Wizard
غير ذلك
مجلدات المشاركة
عملية الفحص
إنشاء اختصار
إعادة التسمية
خصائص



sNipEr AlErT
انذار القناص
Avira AntiVir Personal
AVIRA
Help
Status: Scanning file
Last object:
14.1%
Last detection: No detection!
Virus information
Scanned files: 332
Scanned directories: 89
Scanned archives: 6
Time elapsed: 00:03
Scanned: 14.1%
Detections: 0
Hidden objects: 0
يتم الان فحص القرص سي
لاني محدد القرص سي
Stop
Pause



او لفحص شامل للجهاز هكذا



الآن هل تعتقد انك حميت جهازك بنسبة 100٪ .. لا لايوجد جهاز بهذا العالم محمي 100٪ لكن الحمايه مطلوبه

دعنا نتعمق اكثر في ملفات التجسس هناك اطفال هكرز يقومون بتشفير ملف التجسس طيب انا انسان ما اعرف ماهي او معنى تشفير ملف تجسس

هذا يا طويل العمر شخص قادر وعرف نقاط او القيم المكشوفه بملف التجسس وقام بتشفيرها ليجعل برامج وملفات التجسس غير مكشوفه من الحمايات

طيب لنفرض شخص ارسل لنا ملف من البريد او من محادثة المسن او انك قمت بتحميل ملف من الانترنت كيف نعرف بانه ملف تجسس تابع معي اولا

هناك مواقع تسمى بمواقع الفحص ترفع الملف الذي حملته لموقع الفحص ليتم فحصه من جميع الحمايات فان تم كشف برنامج ما لهذا الملف سيظهر لك

اما اذا لم يكشف بانه ملف مكشوف عليك بان لا تفتح هذا الملف اقل شي لمدة يومين او لثلاثة ايام لانك عندما ترفع ملف لموقع الفحص ولم يتم كشفه

فان القيم التي تم فحصها ستكشف قريبا ومن موقع الفحص يرسل التحديثات لمواقع الحمايه وانت عليك بتحديث برنامج الحمايه فان تم التحديث

وفحصت الملف الذي حملته ولم يجد فيه شي فانه سليم \ لكن هل انه سليم اما لا .. يمكن التحديثات مانزلت \ فانا اقلك يوجد برامج معروفه تظهر لك جميع البرامج التي شغالة بالوندوز

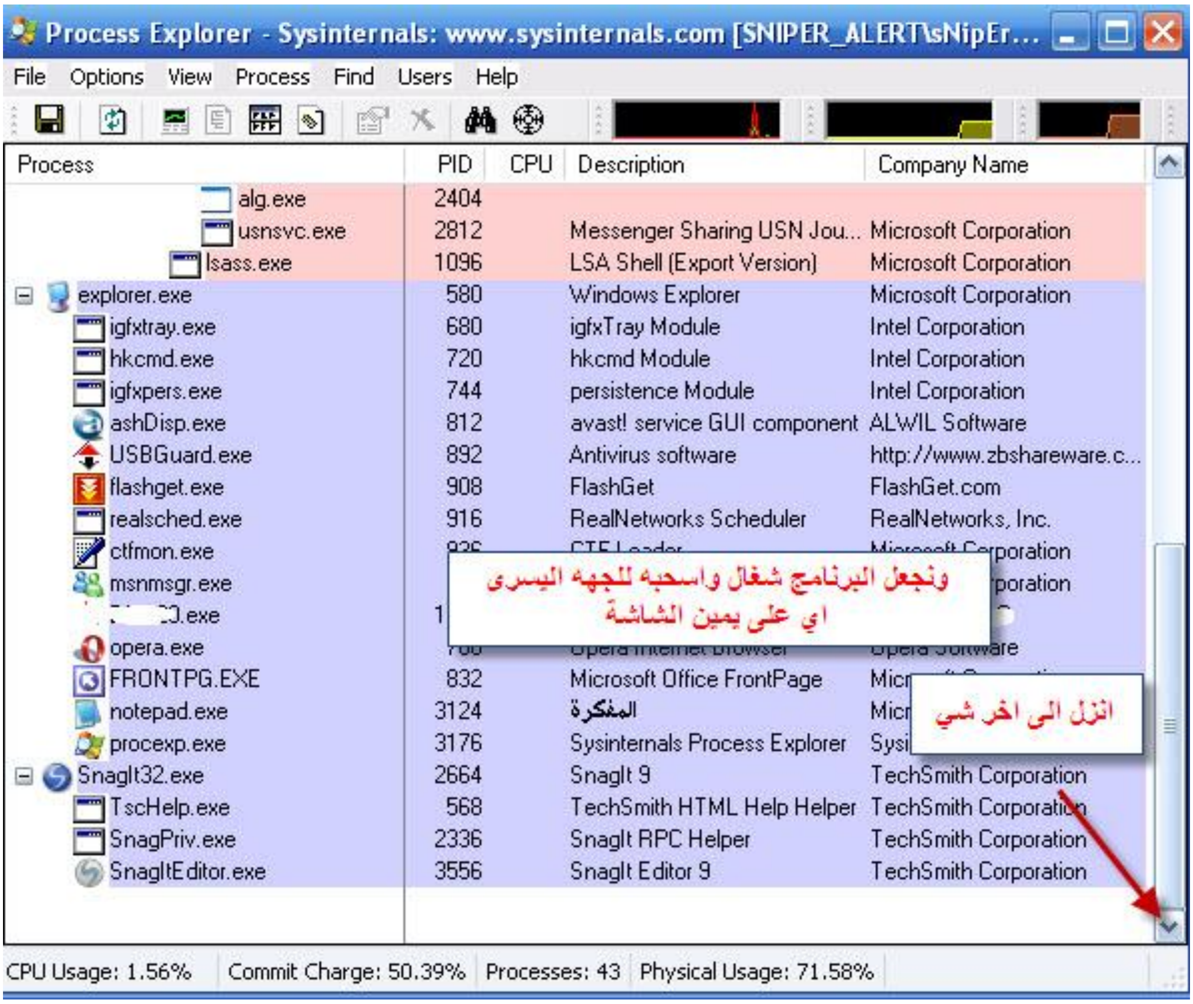
عليك استخدامها \ فعند تشغيل هذا البرنامج اجعله شغال وشغل البرنامج الذي حملته او انك شاك فيه فتجد البرنامج يظهر ما اشتغل في الجهاز ان لاحظت ملف غريب

اشتغل معناته البرنامج مدموج او ملغوم وأنا راح اشرح هذا البرنامج تاااابع معي

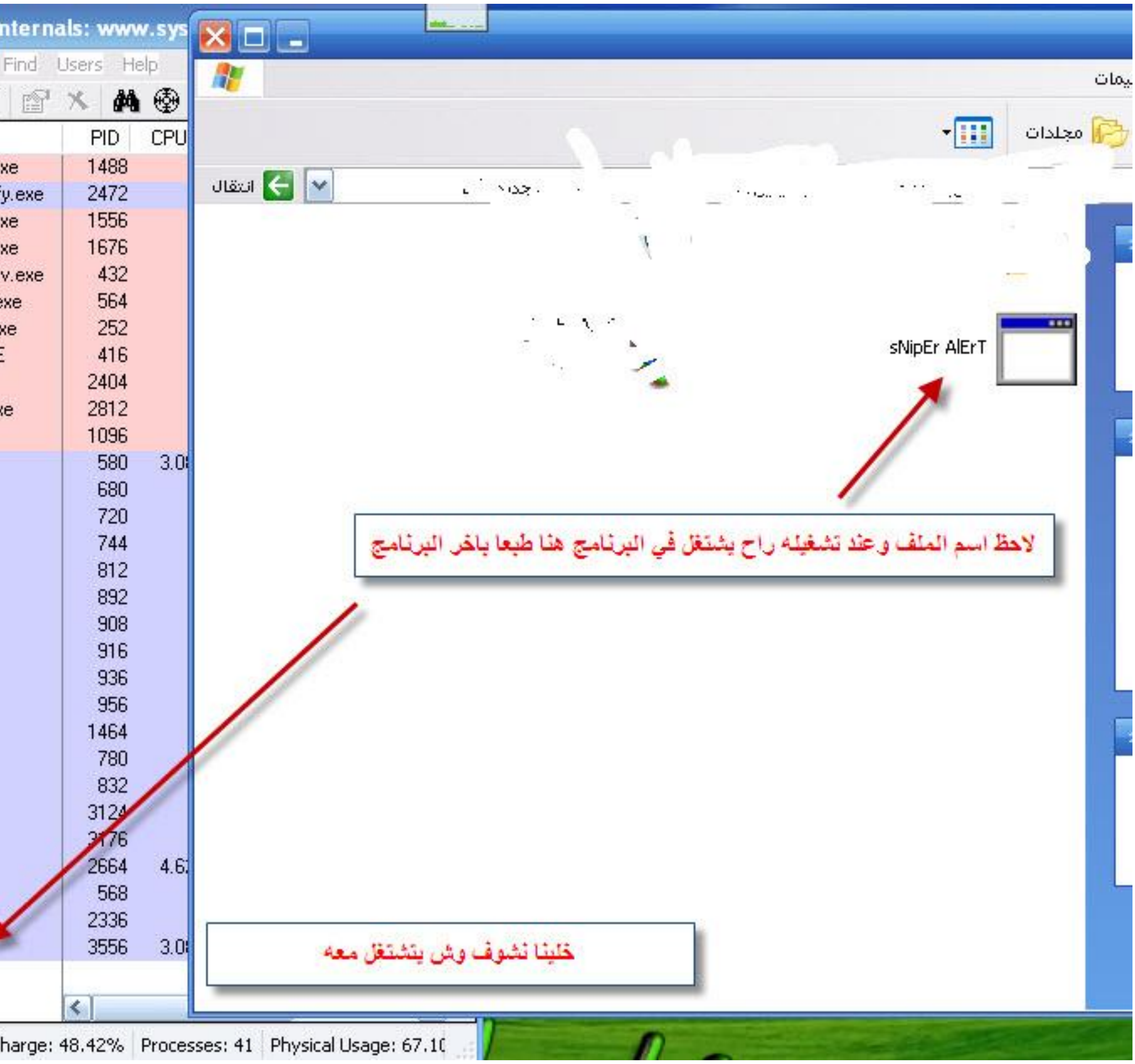
البرنامج اسمه ProcessExplorer

لتحميل البرنامج اضغط هنا

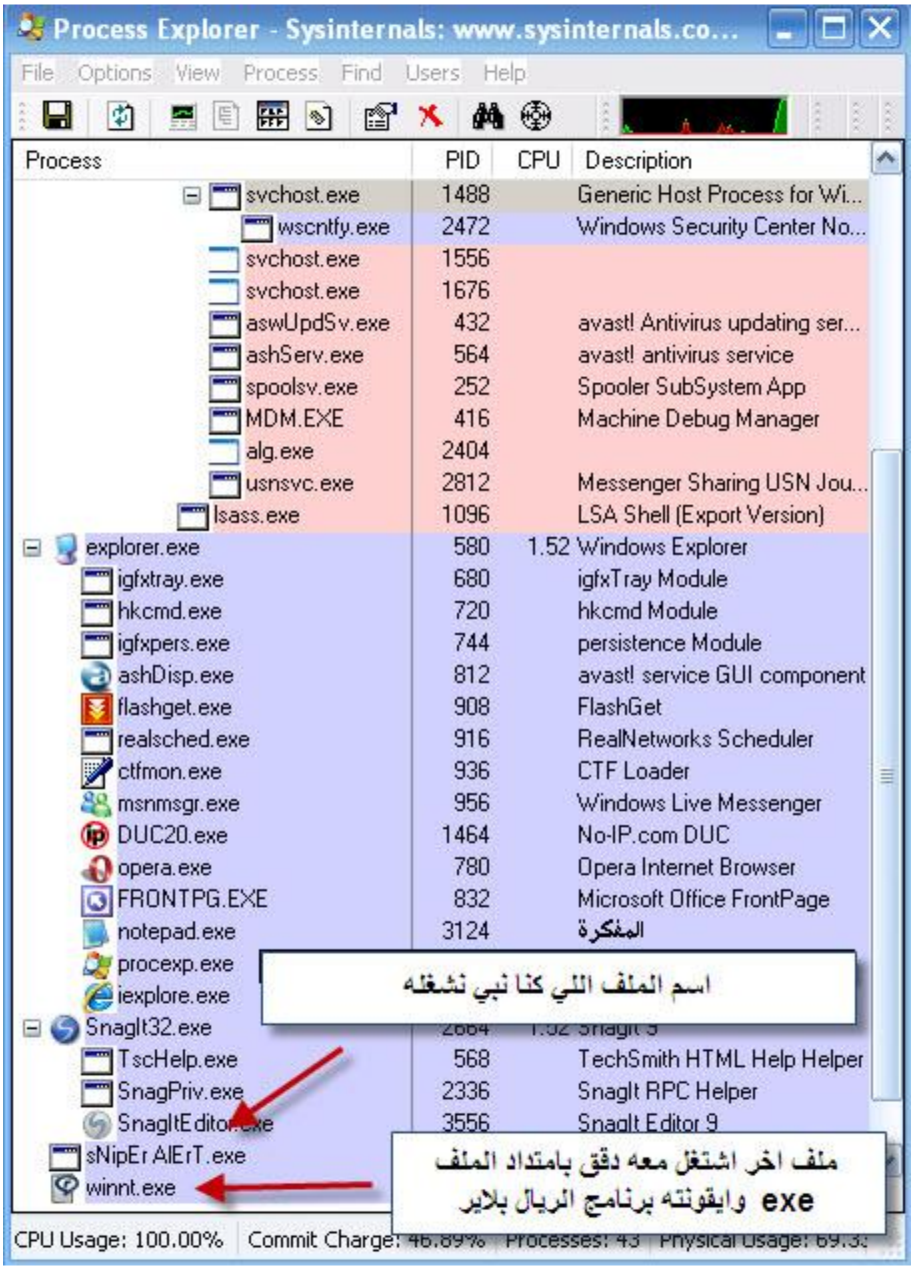
تابع معي كيفية عمل البرنامج



الان نشغل الملف اي ملف مثلا تابع معي كيف نعرف انه مدموج اما لا ؟



sNipEr AlErT
لاحظ اسم الملف وعند تشغيله راح يشتغل في البرنامج هنا طبعا باخر البرنامج
خلينا نشوف وش يتشتغل معه
Processes: 41



الان وش فهمنا من هذه المعلومه ؟

فهمنا اننا شغلنا ملف باسم sNipEr AlErT وعند تشغيل هذا الملف اشتغل معه ملف اخر باسم winnt وكان امتداده exe وشكل ايقونته لبرنامج الريال بلاير

عمرها ماصارت ملف امتداده exe وايقونته ريال بلاير وهذه نقطه مهمه لازم تعرفها بان اطفال الهكرز يغيرون شكل الايقونه وانت تحسبها ايقونه ملف صوتي او فيديو

فعلينا قبل فتح اي ملف نركز بالايقونه الخاصه فيه والامتداد ايضا

طيب عرفنا هذه النقطه طيب ليه ما نحاول نعرف ان هذا الملف مدموج اما لا افظل من اننا نفتح هذا الملف ! تابع معي



اكيد الآن وصلت المعلومه

الان نأتي للحماية التي تجعلك مرتاح البال عن طريق برنامج الديب فريز الشهير المعروف بتجميد النظام - طبعا هذا البرنامج دايم نجده في مقاهي الانترنت

جميل لكن خبيرين الهكرز تمكنو من ايجاد طريقة لتخطي الديب فريز لكن ما يهمنا المهم اننا نحاول بقدر المستطاع حماية جهازنا

فعند تركيب الديب فريز معناتك حميت جهازك بنسبة50 ٪ الى 75 ٪ راح اشرح لكم فكرت البرنامج :

عند تركيب البرنامج فعليك تحديد الاقراص لكي يجمدها لك البرنامج طبعا وش المقصود بالتجميد ؟ المقصود انه عند تركيب البرنامج وانت على النت او تتصفح جهازك وثبت برامج

او صار اي مشكله بالجهاز او مثلا ملف تجسسي فتحته وانت ما تدري فقط عليك اعادة تشغيل الجهاز او اطفائه وعند تشغيل الجهاز يرجع الجهاز الى حالته الطبيعية

كأنك ما فتحت برنامج قبل اخر جلسة لك على الكمبيوتر وحتى لو حذفت ملفات بالغلط فقط اعد تشغيل الجهاز ويرجع كل شي مثل ما كان لنفرض انك

حددت القرص C عند تثبيت الديب فريز فـ اي شي تحذف من القرص سي فقط اعد تشغيل الجهاز ويرجع كل شي مثل ما كان وهكذا على الاقراص الباقيه

بس خذ معلومه انت حميت القرص السي اي شي تحطه بالسي مثل المستندات او سطح المكتب راح يروح من بعد تشغيل الجهاز

يعني لازم تحفظ اي ملف بالقرص الدي لانك حميت القرص السي لكن لو بغيت تحط شي بالمستندات او سطح المكتب لازم تلغي التجميد "" إبطال مفعول التجميد

وكذا تقدر تحط اي شي بس لو بغيت تطفي الجهاز قبل ما تطفيه لازم ترجع تفعل الديب فريز

نقطه مهمه !!

لما تكون مفعل الديب فريز وانت اخترت عند تركيب البرنامج لتجميد القرص سي بانه لا يمكنك إبطال مفعول البرنامج إلا بعد اعادة التشغيل الجهاز ويظهر على ايقونة البرنامج

في اسفل شريط المهام عليه علامة اكس

طيب خلونا نجرب البرنامج : تاااابع معي :

لتحميل البرنامج

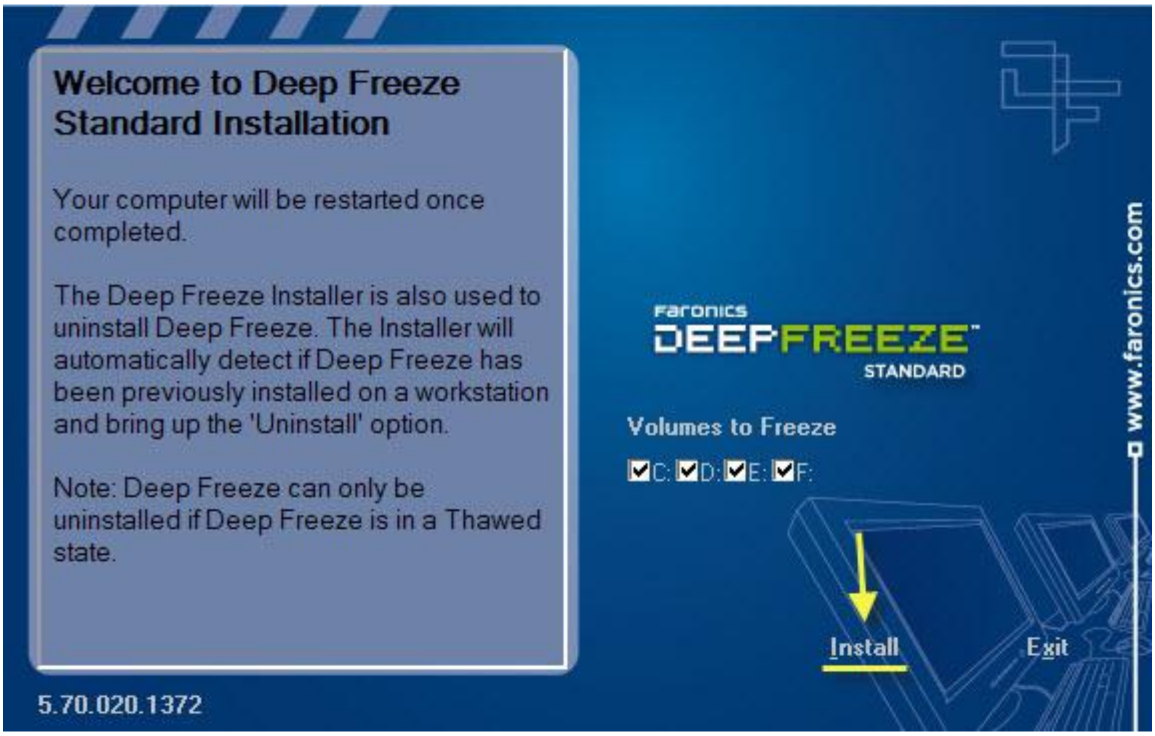
[اضغط هنا]

صورة البرنامج



تابع عملية التثبيت ....!



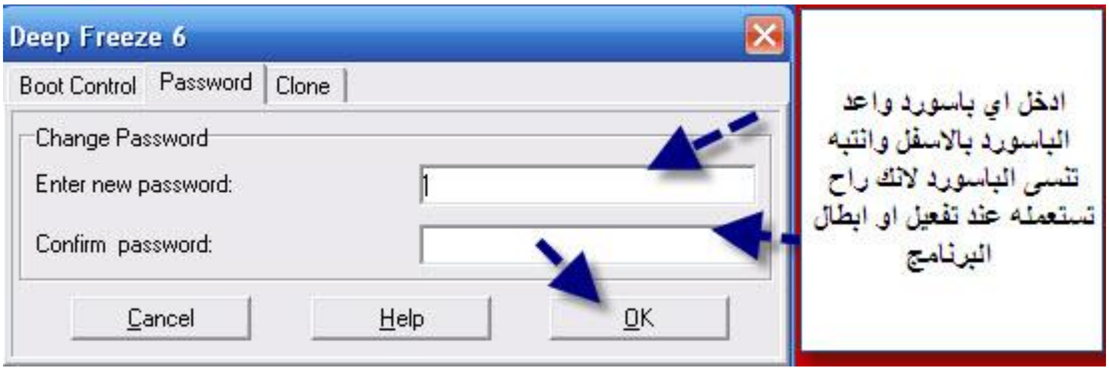


طبعا بالصورة اللي فوق حاطلك اقراص وعلى حسب جهازك \ طبعا هو يخيرك بالاقراص الي تبي تحميها وانت حدد الي تبي تحميه واهم شي القرص السي

يعني حدد على القرص السي وازل علامات الصح من الاقراص الباقيه

انتظر وسوف يعاد تشغيل الجهاز وراح يطلع لك مربع حوار يطلب من الباسورد انظر الى الصورة





الان ستجد البرنامج مفعل في شريط المهام



نلاحظ انه مافي علامة اكس عليه ومعناته انه مجمد القرص اللي انت اخترته

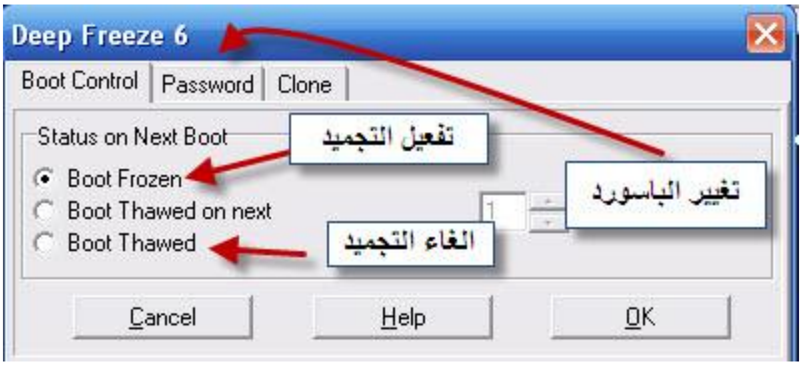
طيب حن جمدنا القرص السي الحين ما نقدر نحفظ اي شي بالسطح المكتب او المستندات او اي شي ندخله بالنت ما راح يحفظه لانه

يحمي القرص السي طيب لو نبي نحفظ ملفات بالسي او بالمستندات لازم نبطل مفعول البرنامج وهو عن طريق الضغط بالكيبورد

ctrl+alt+shift+f6

وراح يطلع معنى اطار يطلب الباسورد نكتب ونضغط اوكي

وتأتينا هذه النافذه



كل مره تفعل او تبطل مفعول البرنامج لازم تعيد التشغيل لان عند ابطال مفعول التجميد واعادة تشغيل الجهاز راح يظهر على الايقونة في شريط المهام عليها علامة اكس

انتهينا ارجو ان فكرة البرنامج واضحه

طيب الان نريد تفادي الوقوع بالاخطاء وهي البريد \ بعض الاحيان يأتي شخص يرسل لك رابط مثلا يقول لك ادخل على الصفحة وضع ايميلك وباسورده

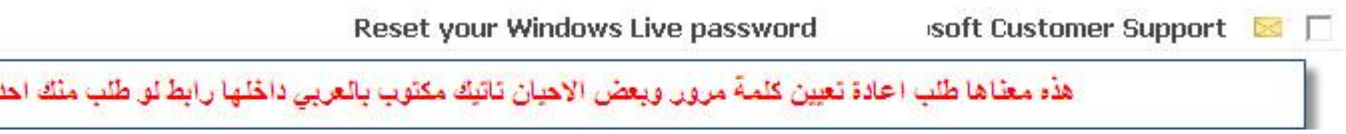
او مثلا يقلك تبي ماسنجرك يصير شكله حلو او من هذا الكلام ...إلخ طبعا يعطيك رابط عند الدخول له تجد صفحة موقع الهوتميل التي تطلب منك ادخل الباسورد والايميل

فهذه نقطه مهمه وهي عبارة عن صفحة مزوره صممها ورفعها على رابط واعطاك هي دقق برابط الذي عطاك \ فأول ما تشوف انه عطاك صفحة ادخلتك على موقع مثل صفة الدخول

للهوتميل فاعرف انها مزوه اياك بالدخول

ايضا هناك احتيالات مثل اعادة تعيين كلمة المرور فيرسل شخص لك اعادة تعيين كلمة المرور ويطلب منك اعاطه الرابط (الوصله) فاول ما تعطيه يدخل على صفحة يغيير

كلمة المرور للإيميل الخاص بك وتأتيك الرساله على الشكل التالي



اخي \ اختي انتبه عند وجود جهازك كاميرا عليك بتغطيتها بوضع قطعة قماش قويه لان بامكان الطفل الهاكر بتصويرك وانت لا تعلم فعند دخولك للانترنت احرص

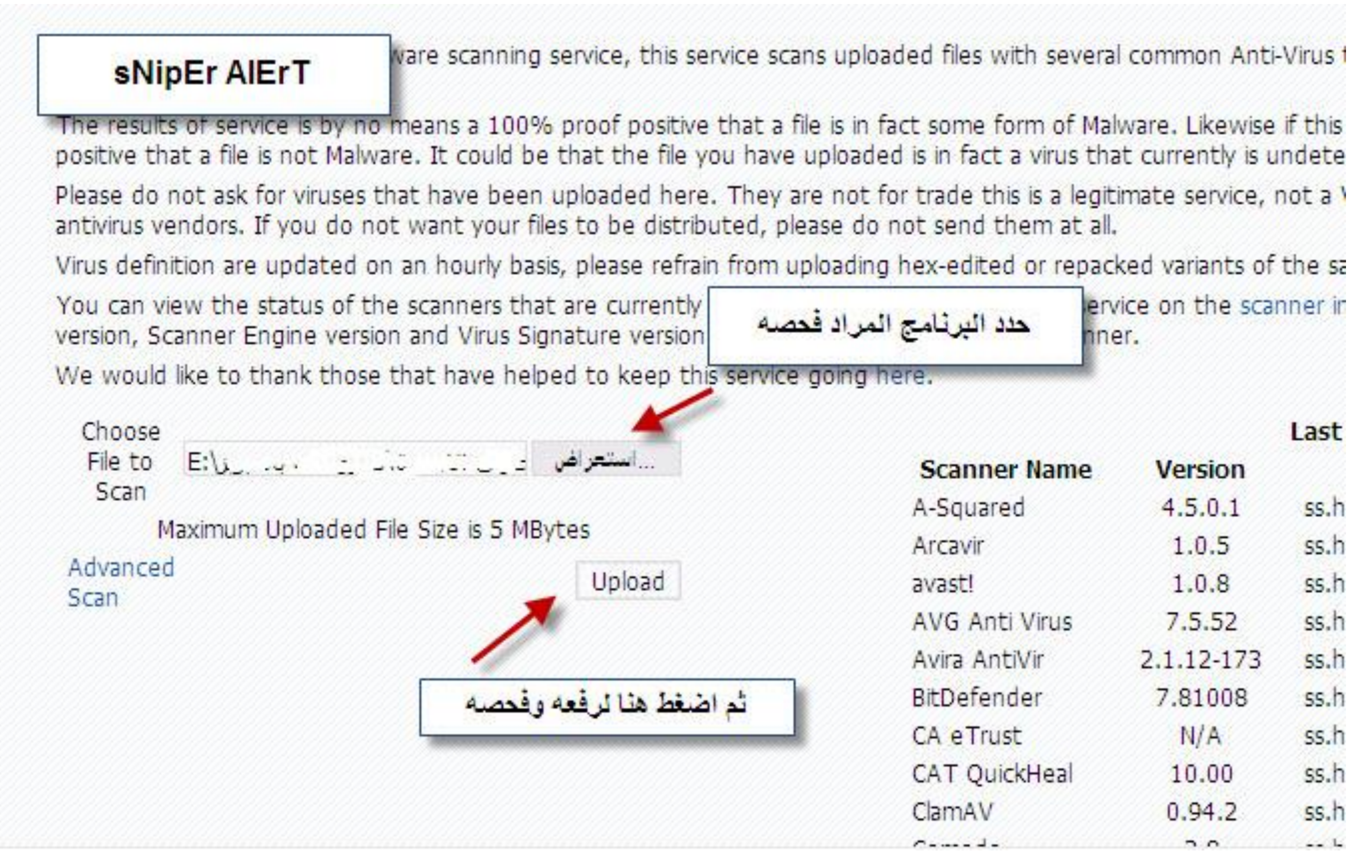
على ان الكاميرا مغطاه

الان ساشرح لكم طريقة الفحص بمواقع الفحص لتعرف هل الملف الذي تريد فحصه هل هو مكشوف من الحمايات اما لا

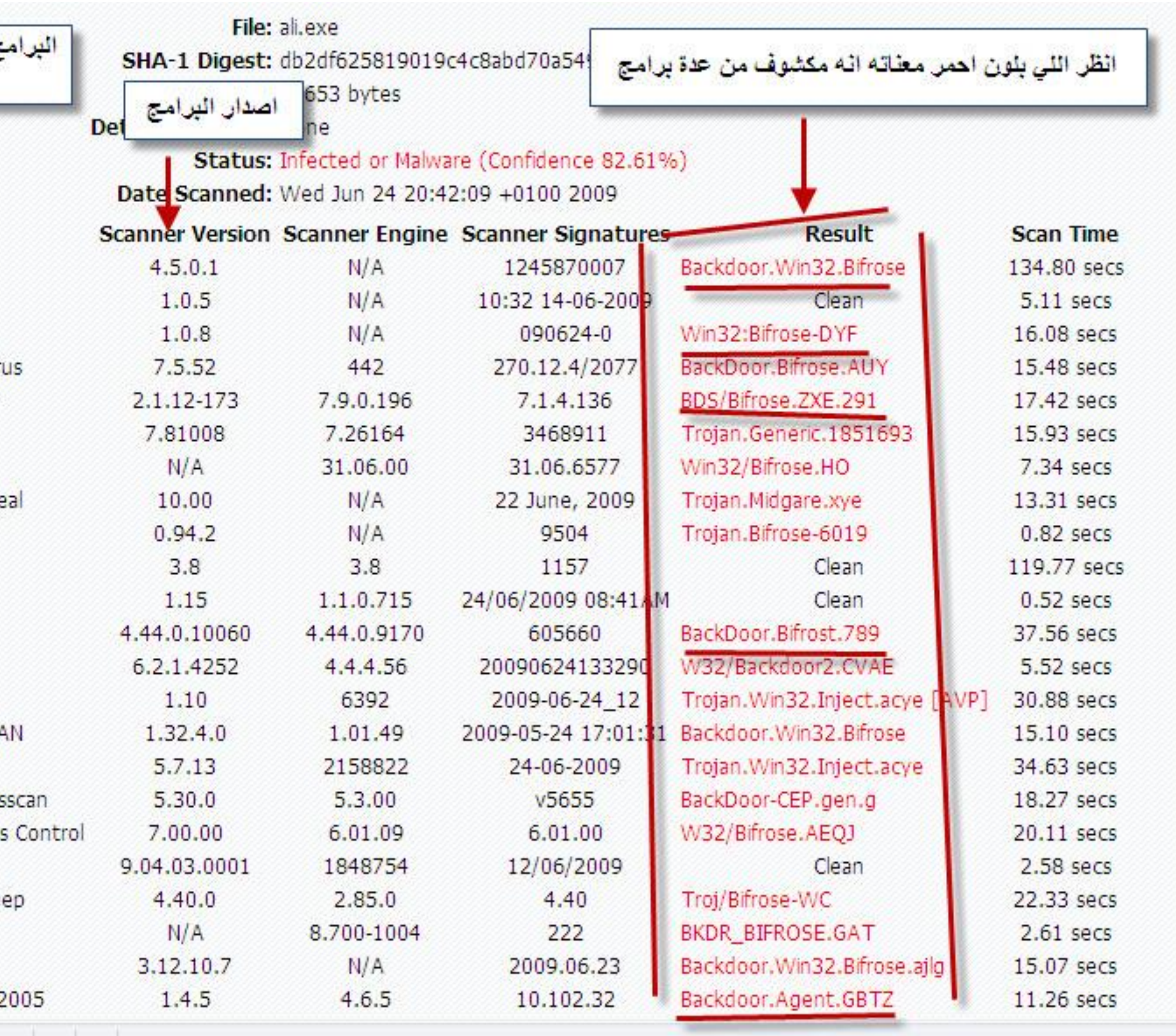
ادخل على هذا الموقع

http://scanner.virus.org/

واتبع الصور




below, you have to the option to have the results of the scan sent to you after the scan has completed. To do this please
s is only kept for the duration of the scan and is then disgarded.
File to
an
استعراض...
Maximum Uploaded File Size is 5 MBytes
ults to:
(enter email address if
required)
Do Not Distribute to Anti Virus
Companies
Upload and Scan
plete
56.02 KB uploaded.
Virus.Org rogue file scanning service is powered by
bitdefender
secure your every bit
AVG Anti-Virus
FRISK
F-Prot
ARCABIT
جاااري الرفع
avast!
VirusBuster
McAfee
F-SECURE
cat
TREND
MICRO
pandasoftware
A-SQUARED
ca
Copyright (c) Virus.org 1997-2009. All Trademarks Acknowledged.
Virus.Org Malware Scanner is Hosted on Wizards Ltd. Network



File: ali.exe
SHA-1 Digest: db2df625819019c4c8abd70a54
653 bytes
Det ne
Status: Infected or Malware (Confidence 82.61%)
Date Scanned: Wed Jun 24 20:42:09 +0100 2009

	Scanner Version	Scanner Engine	Scanner Signatures	Result	Scan Time
	4.5.0.1	N/A	1245870007	Backdoor.Win32.Bifrose	134.80 secs
	1.0.5	N/A	10:32 14-06-2009	Clean	5.11 secs
	1.0.8	N/A	090624-0	Win32:Bifrose-DYF	16.08 secs
rus	7.5.52	442	270.12.4/2077	BackDoor.Bifrose.AUY	15.48 secs
	2.1.12-173	7.9.0.196	7.1.4.136	BDS/Bifrose.ZXE.291	17.42 secs
	7.81008	7.26164	3468911	Trojan.Generic.1851693	15.93 secs
	N/A	31.06.00	31.06.6577	Win32/Bifrose.HO	7.34 secs
eal	10.00	N/A	22 June, 2009	Trojan.Midgare.xye	13.31 secs
	0.94.2	N/A	9504	Trojan.Bifrose-6019	0.82 secs
	3.8	3.8	1157	Clean	119.77 secs
	1.15	1.1.0.715	24/06/2009 08:41AM	Clean	0.52 secs
	4.44.0.10060	4.44.0.9170	605660	BackDoor.Bifrost.789	37.56 secs
	6.2.1.4252	4.4.4.56	20090624133290	W32/Backdoor2.CVAE	5.52 secs
	1.10	6392	2009-06-24_12	Trojan.Win32.Inject.acye [AVP]	30.88 secs
AN	1.32.4.0	1.01.49	2009-05-24 17:01:31	Backdoor.Win32.Bifrose	15.10 secs
	5.7.13	2158822	24-06-2009	Trojan.Win32.Inject.acye	34.63 secs
sscan	5.30.0	5.3.00	v5655	BackDoor-CEP.gen.g	18.27 secs
s Control	7.00.00	6.01.09	6.01.00	W32/Bifrose.AEQJ	20.11 secs
	9.04.03.0001	1848754	12/06/2009	Clean	2.58 secs
ep	4.40.0	2.85.0	4.40	Troj/Bifrose-WC	22.33 secs
	N/A	8.700-1004	222	BKDR_BIFROSE.GAT	2.61 secs
	3.12.10.7	N/A	2009.06.23	Backdoor.Win32.Bifrose.ajlg	15.07 secs
2005	1.4.5	4.6.5	10.102.32	Backdoor.Agent.GBTZ	11.26 secs

استرجع ايميلك المسروق من شركة الهوت ميل

المصدر ترياق العرب

الكاتب :AlQaTaRi

بسم الله الرحمن الرحيم

السلام عليكم اخواني الغاليين اعضاء ترياق العرب

من يومين انا واخوي الغالي SnIpEr_h **قلت له نبي نجرب طريقه نسترجع ايميلاتنا من الهوت ميل اذا انسرقت لاقدر الله**

قلت له ارسل لي موقع الدعم الفني للهوت ميل ودخلت ايميل عندي قديم وخزنت كل البيانات المهمه

وقلت لاخوي SnIpEr_h **يدخل الايميل ويغير كل بياناته وكل شي في الايميل وانا براسل الشركه**

المهم راسلت الشركه خلال 24 **ساعه ردو علي برساله قالو لي كل معلوماتك صحيحه**

وارسلو لي رساله ثانيه فيها طلب استعادة الباسورد خلونا نتابع الشرح بالصور كيف نخزن البيانات والى استرجاع الايميل

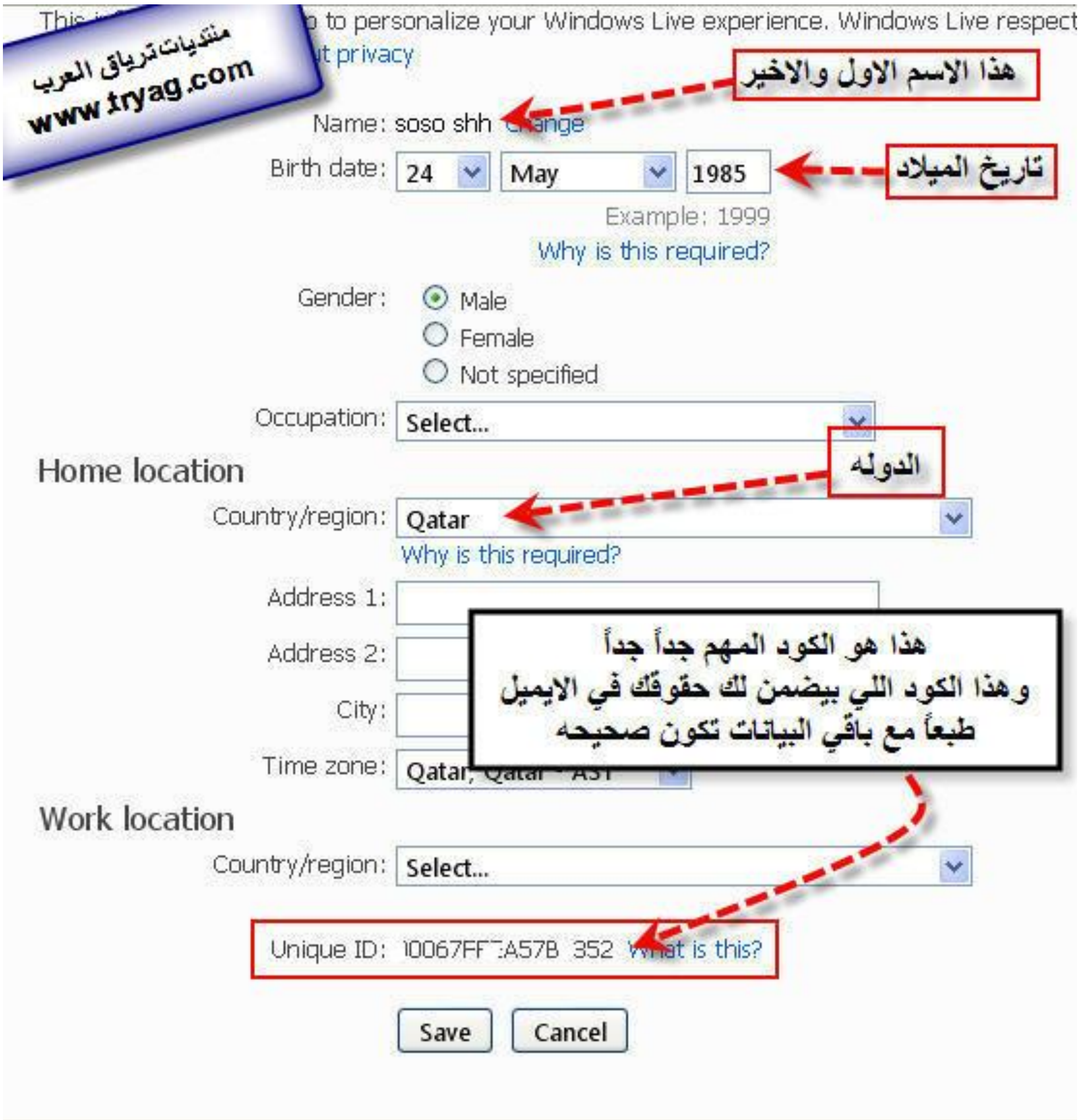
طبعاً الشرح مفصله تفصيل حتى اللي بعضهم تلاقيه مايعرف يدخل على معلوماته ويسجلها تابعو معاي

ادخل على ايميلك وبعدها ندخل على الاوبشن مثل هالصوره


ive Hotmail
منتديات ترياق العرب
www.tryag.com
soso
sign out
1
Options
Language
Search your e-
English
Themes
get to
More themes
More options
2
ندخل على Options
ونختار اخر شي
More Options
3 days ago


اضغط هنا
Manage your account
View and edit your personal information
Send and receive mail from other e-mail accounts
Forward mail to another e-mail account
Send automated vacation replies
منتديات ترياق العرب
www.tryag.com


هذي بيانات الايميل نخزنها كلها في ملف في الجهاز
او على سي دي او يو اس بي داخل ملف txt
لاستخراج كافة البيانات اضغط على
Registered information
soso shh
[redacted]@hotmail.com
Registered since: 23 March 2008
Country/region: Saudi Arabia
Birth date: 24 May 1985
Registered information
Password reset information
Password: ****** Change
Question: Name of first pet Change
Alternate e-mail address: [redacted] Change
Mobile number and PIN: Not specified Add
منتديات ترياق العرب
www.tryag.com


منتديات ترياق العرب
www.tryag.com
to personalize your Windows Live experience. Windows Live respect
privacy
هذا الاسم الاول والاخير
Name: soso shh Change
Birth date: 24 May 1985
تاريخ الميلاد
Example: 1999
Why is this required?
Gender: Male
Female
Not specified
Occupation: Select...
Home location
الدوله
Country/region: Qatar
Why is this required?
Address 1:
Address 2:
City:
Time zone:
هذا هو الكود المهم جداً جداً
وهذا الكود اللي يضمن لك حقوقك في الايميل
طبعاً مع باقي البيانات تكون صحيحه
Work location
Country/region: Select...
Unique ID: What is this?
Save
Cancel


منتديات ترياق العرب
www.tryag.com
Delete Junk
Mark as
Move to
Sort by
Drafts
Sent
Deleted (3)
Manage folders
نـدخل على قائمة الاتصالات اللي فيها كل
الايميلات اللي ضايفينها
Related places
Today
messages
Contact list
Calendar

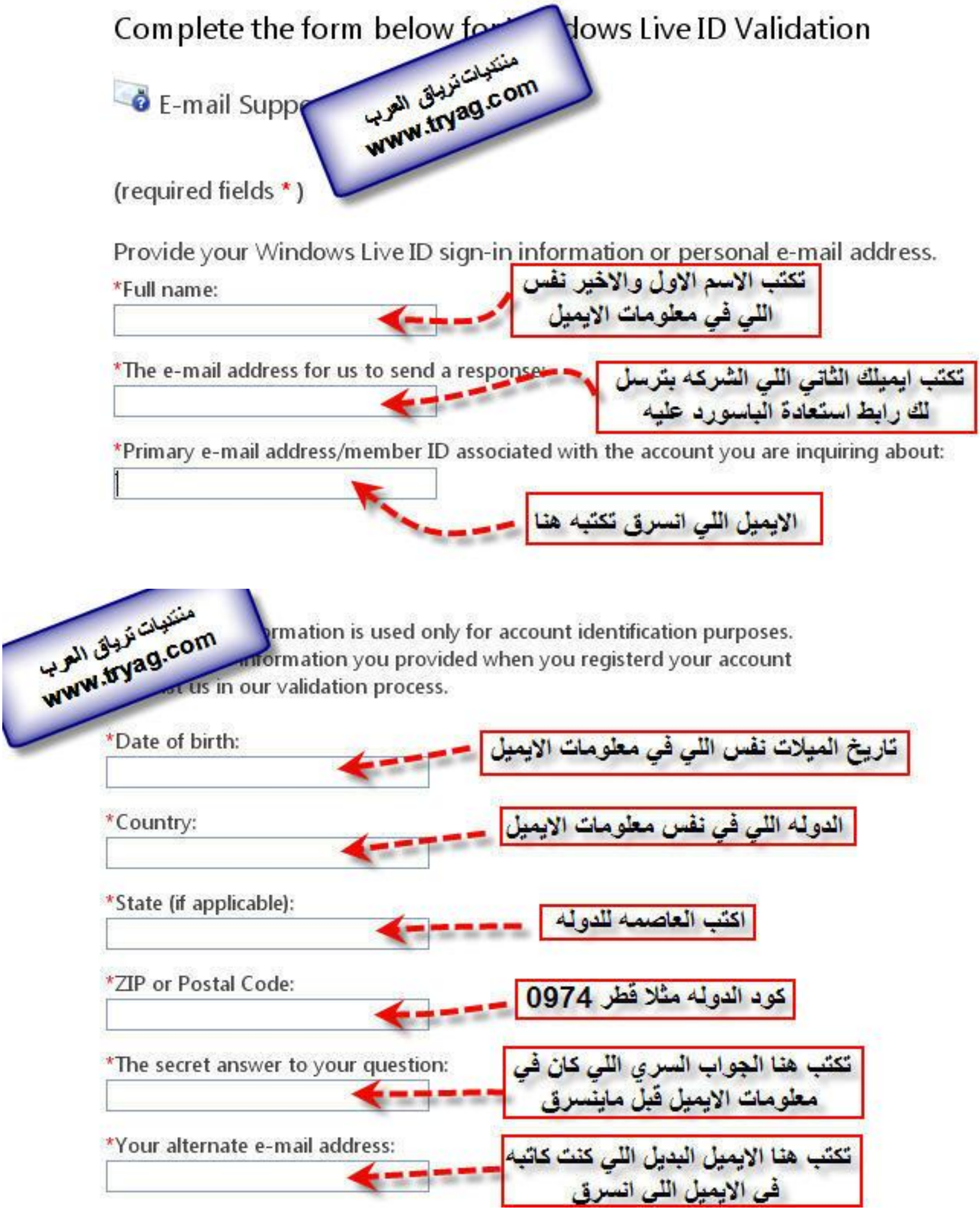
الان بـكـذا خـزنا المعـلـومات المهـمه واحـفـظـها عـنـدك في مـلـف نصـيtxt خـارج الجـهـاز عـلـى يو اس بي او سـي دي

المهـم الان لـو انسـرق ايمـيلك لاقدر اللّه ماعـليـك الا انك تـدخـل هالموقـع الخـاص بـالـدعـم الـفـنـي وتراسـلـهـم

[&https://support.live.com/eform.aspx?productKey=wlidvalidation ct=eformcs](https://support.live.com/eform.aspx?productKey=wlidvalidation&ct=eformcs)

وهـذا الشـرح الخـاص بـالـدعـم الـفـنـي




Complete the form below fo... dows Live ID Validation

منتديات ترياق العرب
www.tryag.com

E-mail Supp...

(required fields *)

Provide your Windows Live ID sign-in information or personal e-mail address.

*Full name:

تكتب الاسم الاول والاخير نفس اللي في معلومات الايميل

*The e-mail address for us to send a response:

تكتب ايميلك الثاني اللي الشركه بترسل لك رابط استعادة الباسورد عليه

*Primary e-mail address/member ID associated with the account you are inquiring about:

الايميل اللي انسرق تكتبه هنا

منتديات ترياق العرب
www.tryag.com

...rmation is used only for account identification purposes.
...nformation you provided when you registerd your account
...us in our validation process.

*Date of birth:

تاريخ الميلاد نفس اللي في معلومات الايميل

*Country:

الدوله اللي في نفس معلومات الايميل

*State (if applicable):

اكتب العاصمه للدوله

*ZIP or Postal Code:

كود الدوله مثلا قطر 0974

*The secret answer to your question:

تكتب هنا الجواب السري اللي كان في معلومات الايميل قبلماينسرق

*Your alternate e-mail address:

تكتب هنا الايميل البديل اللي كنت كاتبه فى الايميل اللى انسرق

في هالصوره مكان ماترسل للشركه الرساله حاول انك تكتب كل شي تعرفه عن ايميلك

لاتكتفي بالكلام اللي انا كاتبه مثلا اكتب على الاقل5 او 7 ايميلات انت

ضايفهم

اكتب باسوردك القديم اي شي تعرفه عن ايميلك اكتبه لان يفيدك كثير في استرجاع البيانات


*Your IP address (list the IP addresses from each computer that you use to access your account. To determine your IP address, visit http://www.whatismyip.com The numbers that appear at the top of this Web page are your IP address.)

اول حاجه ندخل الرابط اللي مضلل باللون الاصفر
وبعدين اكتب رقم الاي بي الخاص فيك في المستطيل

*Your Internet service provider (home or work):

اكتب في المستطيل home

*The last date and time that you successfully signed in:

اكتب اخر تاريخ واخر وقت دخلت فيه الايميل المسروق

For Windows Live Hotmail customers:

The names of any folders that you created in addition to the default folders:

اذا كنت مسوي مجلد في الايميل اللي انسرق
اكتب اسم المجلد واذا ماكتبت اتركه فاضي

Names of contacts in your Hotmail address book:

اسم قائمة المتصلين لو كنت كاتبها في
الايميل وليست مهمه

Subjects of any old mail that is in your Hotmail Inbox or mail folders:

وهذا الخيار ليس مهم اتركه فاضي

منتديات ترياق العرب
www.tryag.com

For Windows Live Messenger customers:

Names of contacts on your Messenger contact list:

اسم القائمه اللي في الماسنجر مثلا قائمة الاصدقاء او العائله
واكتب عدد الايميلات في كل قائمه لو كنت عارفهم

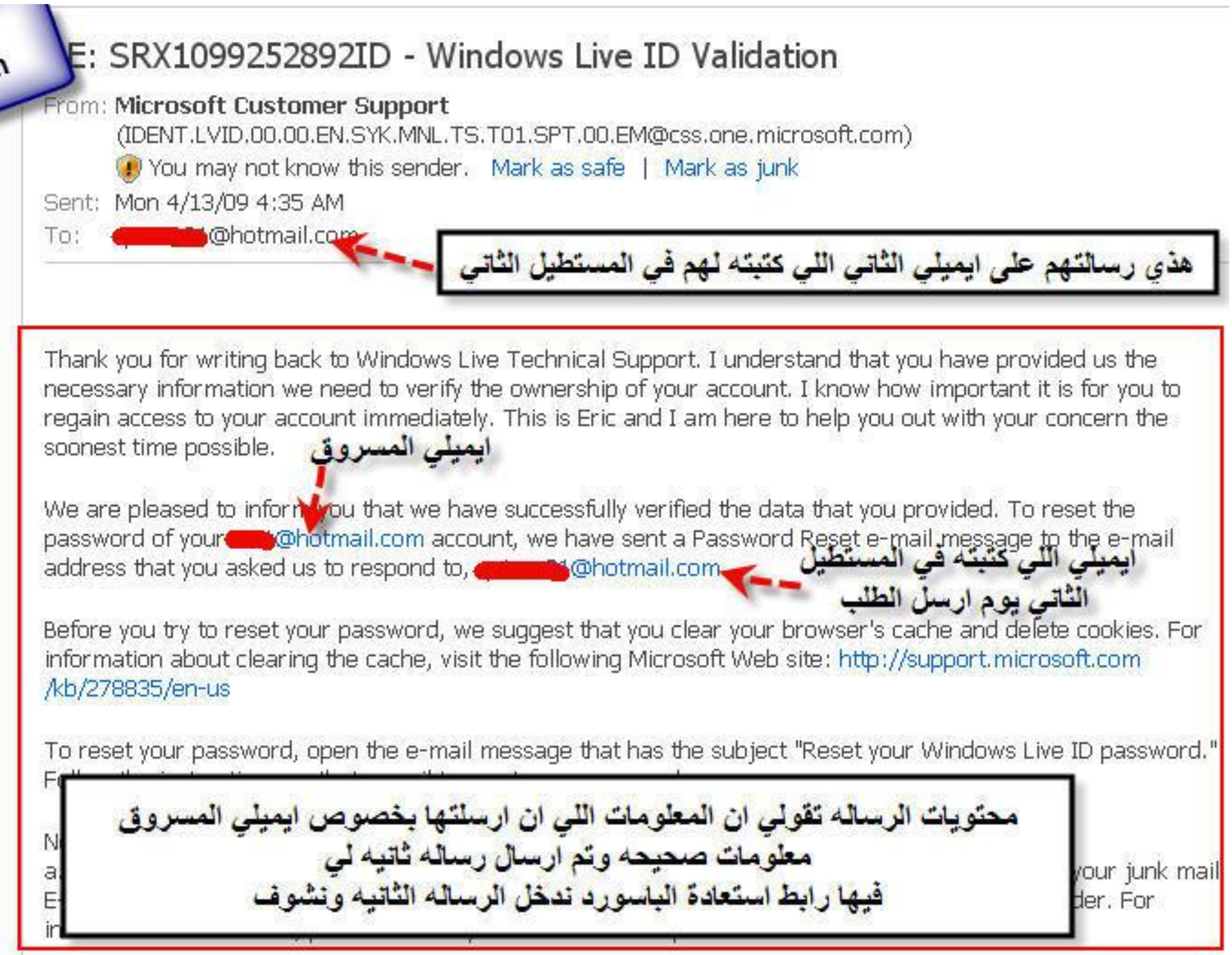
Your Messenger nickname (display name):

اكتب النك نيم اللي في الماسنجر للايميل المسروق


منتديات ترياق العرب
www.tryag.com
Xbox or Zune prepaid card number (The prepaid card information must match the Live ID that you used to sign up.):
Last 4 digits of the credit card used for services:
خيارات ليسة مهمه فقط للي كاتب بيانات الفيزا كارت والكردت كارت الخاص فيه في بيانات الايميل لم استخدمها في استرجاع ايميلي
Expiration of the credit card used for services:
Name as it appears on the credit card used for services:
Any additional info that might be useful in validating the ownership of the account:
هنا نكتب رساله بالانجليزي للشركه ونقول فيها ان تم سرقة ايميلي ولا استطيع استرجاع ايميلي ونكتب لهم الكود اللي في معلومات الايميل هذا وهو وكل ايميل مختلف عن الثاني
Unique ID : 00067FFEA57B9852
في الاخير نضغط على
Submit
By submitting this information, you acknowledge it will be handled in accordance with the terms of the privacy statement.
Privacy Statement
Submit


منتديات ترياق العرب
www.tryag.com
acting Window
Support
هنا يقولك تم ارسال رسالتك وخلال 24 ساعه سيتم الرد عليك
Thank you for submitting your issue to Support.
Your Support Ticket Number: **1099428277**
ticket number. Use this
هذا رقم التذكره الخاصه فيك بالمشكله اللي راسلت فيها الشركه احتفظ في الرقم لو تاخرو على الرد عليك ترسل لهم رقم التذكره الخاص فيك لان كل رساله ولها رقم تذكره مختلفه عن الاخرى
"microsoft.com" domain to
box" within 24 hours, check





E: SRX1099252892ID - Windows Live ID Validation

From: **Microsoft Customer Support** (IDENT.LVID.00.00.EN.SYK.MNL.TS.T01.SPT.00.EM@css.one.microsoft.com)

You may not know this sender. Mark as safe | Mark as junk

Sent: Mon 4/13/09 4:35 AM

To: [redacted]@hotmail.com

هذي رسالتهم على ايميلي الثاني اللي كتبته لهم في المستطيل الثاني

Thank you for writing back to Windows Live Technical Support. I understand that you have provided us the necessary information we need to verify the ownership of your account. I know how important it is for you to regain access to your account immediately. This is Eric and I am here to help you out with your concern the soonest time possible.

ايميلي المسروق

We are pleased to inform you that we have successfully verified the data that you provided. To reset the password of your [redacted]@hotmail.com account, we have sent a Password Reset e-mail message to the e-mail address that you asked us to respond to, [redacted]@hotmail.com

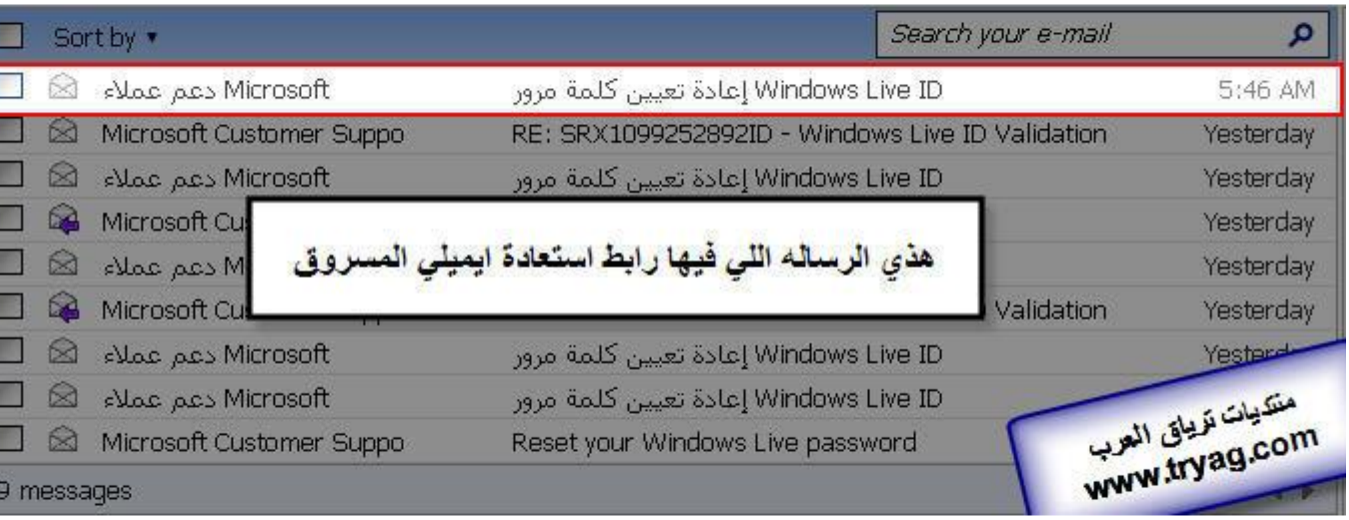
ايميلي اللي كتبته في المستطيل الثاني يوم ارسل الطلب

Before you try to reset your password, we suggest that you clear your browser's cache and delete cookies. For information about clearing the cache, visit the following Microsoft Web site: http://support.microsoft.com/kb/278835/en-us

To reset your password, open the e-mail message that has the subject "Reset your Windows Live ID password."

محتويات الرساله تقولي ان المعلومات اللي ان ارسلتها بخصوص ايميلي المسروق معلومات صحيحه وتم ارسال رساله ثانيه لي فيها رابط استعادة الباسورد ندخل الرساله الثانيه ونشوف

your junk mail
der. For





وفي اخر رساله تضغط على الرابط يطلع لك ايميلك المسروق مكتوب لك في الصفحه

وماعليك الا انك تكتب الباسورد الجديد للايميل الخاص فيك مرتين

وبعدها تدخل على الايميل وتغير كل المعلومات اللي غيرها السارق

الان نقوم بتنظيف جهازنا من الملفات الغير مرغوبه نبدأ باهم مجلد

اولا ندخل للقرص السي ثم مجلد Documents and Settings

سنجد مجلدات نحن نريد مجلد واحد لكن هو مخفي علينا باظهاره

نذهب للوحة التحكم ثم خيارات مجلد ونسوي مثل اللي بالصورة



طيب جميل الان ظهر لنا مجلد مخفي بس هل المجلد المخفي هو اللي نبيه ؟

عشان نتأكد نحن نبي مجلد باسم حسابنا الكمبيوتر الي داخلين عله يسمى حساب مستخدمين اي اليوزر اللي داخلين منه في نظامنا

كيف نعرف تاااابع معي .. ادخل على ادارة المهام



انا حسابي ظاهر لكن انت وش راح يطلع اسم حسابك المهم اللي يطلع لنا هنا في الصورة هو اللي ندخل عليه المجلد

نفرض دخلنا عليه على طول نتوجه الى هذا المجلد Contacts **ونمسح اللي بداخله كله وهذا المجلد خاص بالماسنجر وتذكر نقطه مهمه**

عند دخولك للماسنجر لا تحفظ بياناتك ابد الله يعينك كل ما تدخل اكتب ايميلك وباسوردك

الحين ندخل مجلد Local Settings

نجد بداخله مجلد باسم Temp **نمسح كل اللي بداخله طبعا الطريقة اللي انا مسويها دايم تسويها من ثلاث ايام الى اربع ايام**

طيب مجلد temp **فيه بعض الملفات ما تنحذف انت احذف اللي تقدر عليه**

طيب ننتقل لمجلد اخر في نفس مجلد Local Settings

واسمه Temporary Internet Files **ونمسح كل اللي بداخله**

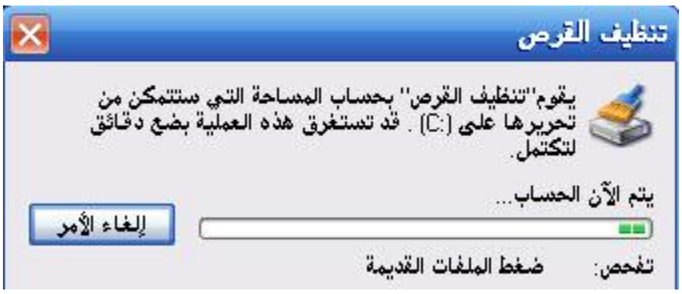
طيب جميييييييييل جدا الحين نروح للقرص السي نجد مجلد باسم windows

ندخل عليه بنلقى مجلد اسمه temp **ايضا نسمح كل شي فيه ولي ما ينمسح نتركه**

الان عملية تنظيف الاقراص

نذهب ابدأ + برامج + برامج ملحقه + ادوات النظام + تنظيف القرص







ننتقل لأهم الاشياء

وهي قفل البورتات وتأكد انك متصل بالانترنت

نذهب لموجة الاوامر

ابدأ + برامج + برامج ملحقه + موجة الاوامر

راح تفتح معنى شاشة سوداء طبعا لازم يكون النت شغال

نبدأ نكتب بالترتيب

ping host

ثم انتر

ping port

ثم انتر

ping port1027

ثم انتر

ping port80

ثم انتر

ping proxy

ثم انتر

ping port

ثم انتر

exit

ثم انتر

الآن نقوم بحذف ملفات خلفها الانترنت

طبعا اخي \ اختي : عند فعل الاشياء التي وضعتها بالكتاب ولديك برنامج الديب فريز لازم يكون على ايقونة الديب فريز علامة اكس

يعني انت موقف التجميد

الان نضغط كليك يمين على متصفح الاكسبلور ونختر خصائص راح تظهر لنا اطار نختر حذف ملفات تعريف الارتباط (اذا كان متصفحك اصداره السادس)

اما اذا كان متصفح اصدار السابع او الثامن نفعل مثل اللي بالصورة


خصائص إنترنت
sNipEr AlErT
انذار القناص
عام
الأمان
خيارات متقدمة
الصفحة الرئيسي
لإنشاء علامات تبويب للصفحات الرئيسية، اكتب كل عنوان على السطر الخاص به.
http://www.google.com
استخدام الحالية
استخدام الافتراضي
استخدام الفارغة
محفوظات الاستعراض
حذف الملفات المؤقتة والمحفوظات وملفات تعريف الارتباط وكلمات المرور المحفوظة ومعلومات نماذج ويب.
حذف...
إعدادات
بحث
تغيير افتراضيات البحث.
إعدادات
نختار حذف
علامات التبويب
تغيير كيفية عرض صفحات ويب في علامات التبويب.
إعدادات
المظهر
الألوان
اللغات
الخطوط
الوصول
موافق
إلغاء الأمر
تطبيق

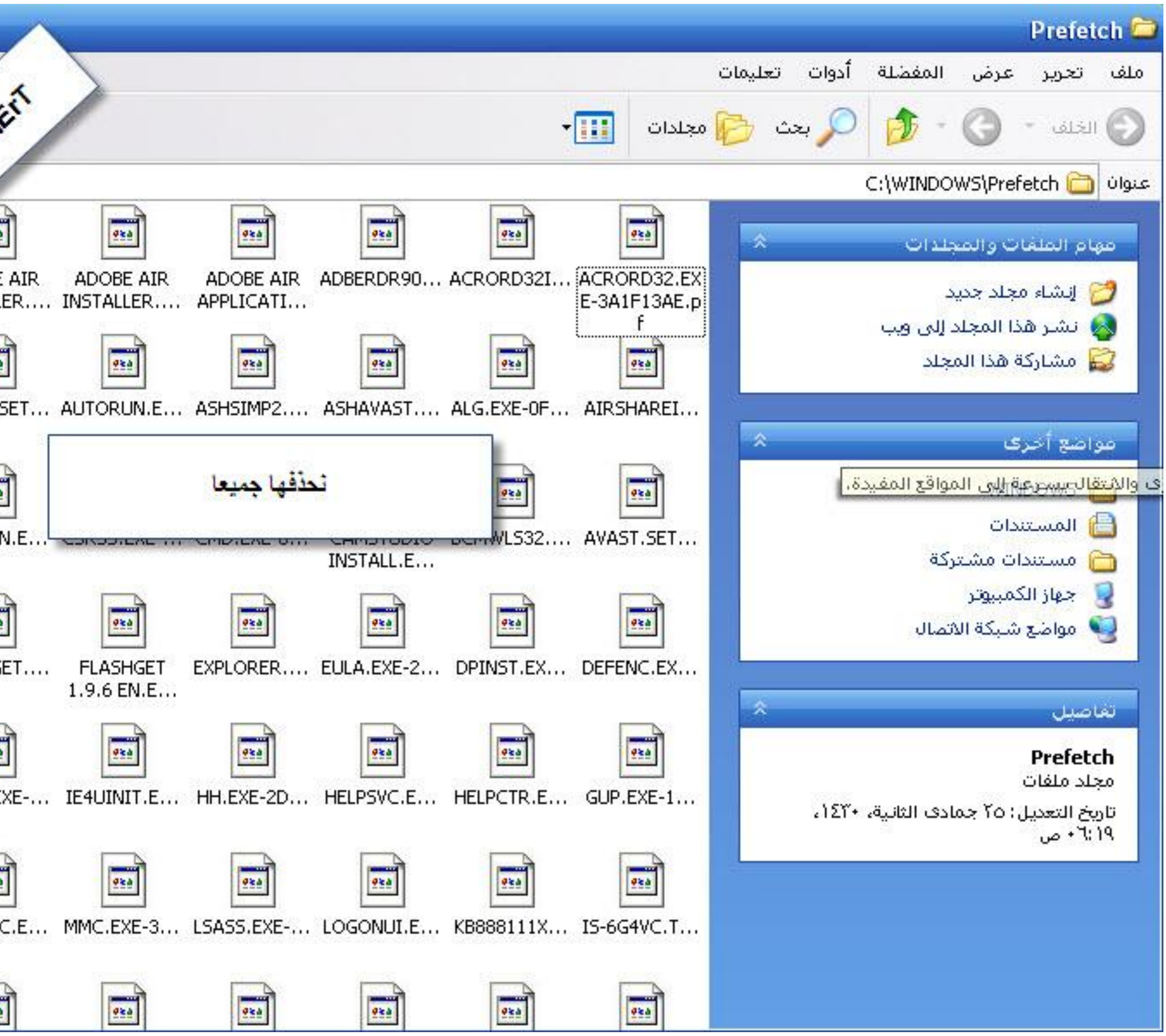

حذف محفوظات الاستعراض
ملفات إنترنت المؤقتة
نسخ صفحات ويب والصور والوسائط التي تم حفظها للعرض بشكل أسرع.
حذف الملفات...
ملفات تعريف الارتباط
ملفات تم تخزينها على الكمبيوتر من قبل مواقع
تسجيل الدخول.
حذف ملفات تعريف الارتباط...
جميع الازرار اضغط عليها او اضغط حذف الكل من هنا
حذف المحفوظات...
حذف النماذج...
كلمات المرور
كلمات المرور التي تم تعبئتها تلقائياً عند تسجيل الدخول إلى موقع ويب قمت بزيارته مسبقاً.
حذف كلمات المرور...
حول حذف محفوظات الاستعراض
حذف الكل...
إغلاق


خصائص إنترنت
sNipEr AlErT
عام
الأمان
الخصوصية
المحتوى
الاتصالات
البرامج
مرشد المحتويات
على هذا الكمبيوتر.
إعدادات
تمكين...
الشهادات
استخدام الشهادات للاتصالات المشفرة والتعرف على الهوية.
مسح حالة SSL
الشهادات
الناشرون
إكمال تلقائي
يقوم الإكمال التلقائي بتخزين الإدخالات
السابقة على صفحات ويب واقتراح
مطابقات.
إعدادات
موجز ويب
إعدادات
اضغط هنا
موافق
إلغاء الأمر
تطبيق



الان نذهب الى ابدأ ثم تشغيل ونكتب : prefetch





الان وضعت لكم ملفات خاصه بالريجستر جميله جدا لكن وضعت المهمه لكم

لتحميل هذه الملفات اضغط هنا



تجد بكل مجلد ملف بهذا الشكل (استعملها كلها)



فقط اضغط عليه ويأتيك مربع حوار





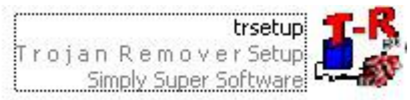
طيب حن مانبي نفرمت الجهاز لان تكلفته غاليه ولا لنا علم بفرمتة الاجهزة وجهازنا مصاب بفايروس

وعند تحميل او تشغيل برنامج حمايه يقوم الفايروس بـ إغلاقه ما العمل ؟

هناك برنامج جميل جدا اسمه Trojan Remover ميزاته جميله قم بتحميله

من هذا الرابط اضغط هنا

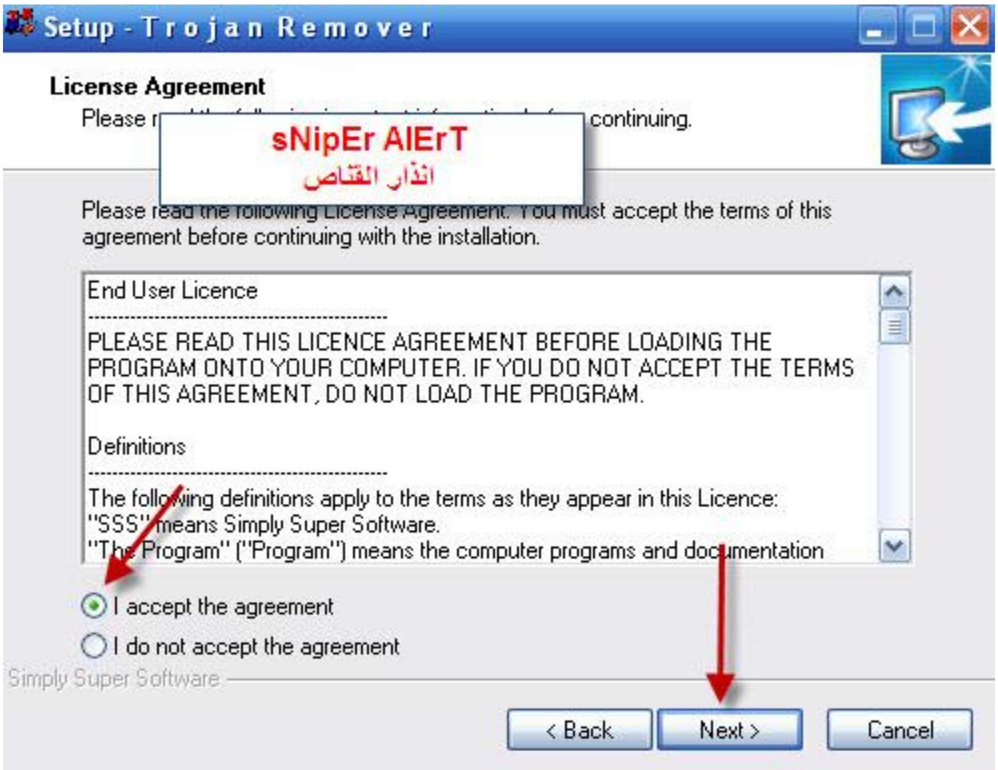
الان قم بحذف برنامج الحمايه الذي بجهازك



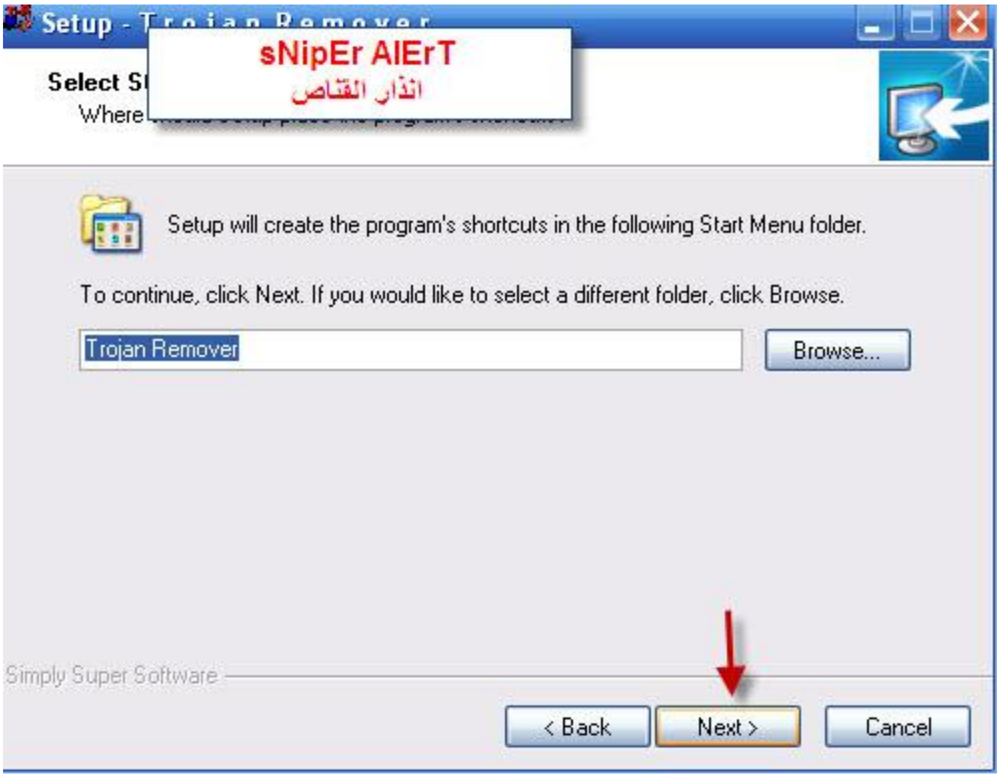
نضغط على البرنامج لتنصيب تابع معي : طبعا الكراك معه مرفق






Setup - T r o j a n R e m o v e r
License Agreement
sNipEr AlErT
انذار القناص
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
End User Licence
PLEASE READ THIS LICENCE AGREEMENT BEFORE LOADING THE PROGRAM ONTO YOUR COMPUTER. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, DO NOT LOAD THE PROGRAM.
Definitions
The following definitions apply to the terms as they appear in this Licence:
"SSS" means Simply Super Software.
"The Program" ("Program") means the computer programs and documentation
I accept the agreement
I do not accept the agreement
Simply Super Software
< Back
Next >
Cancel

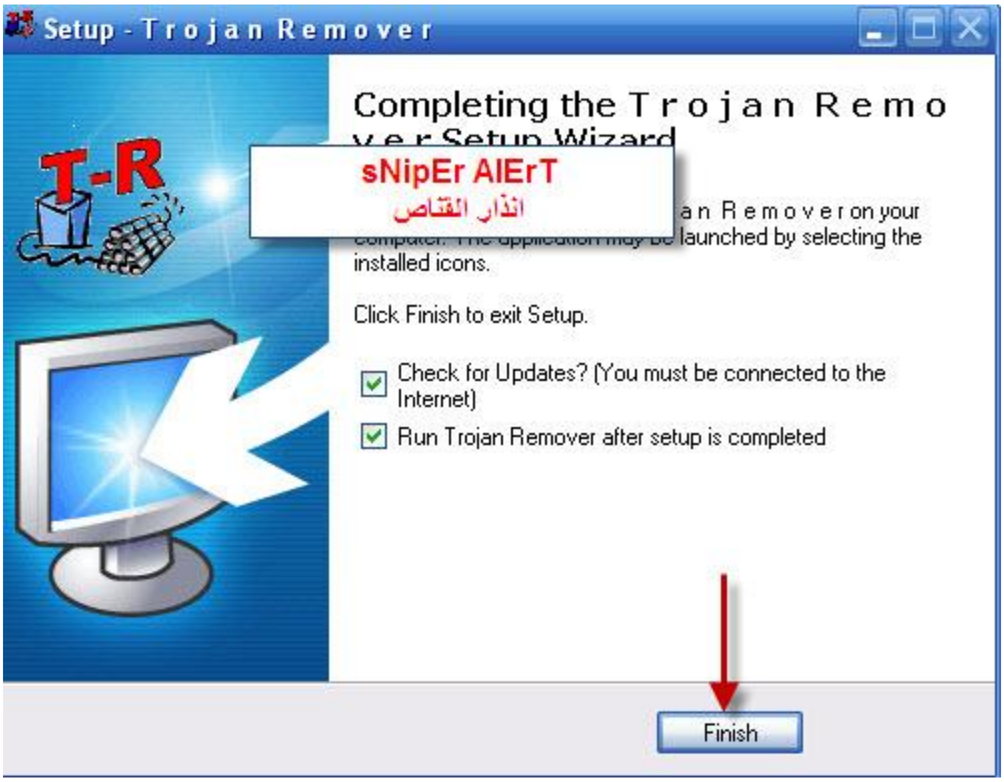

Setup - T r o j a n R e m o v e r
Select Destinatio
sNipEr AlErT
انذار القناص
Setup will install T r o j a n R e m o v e r into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\Trojan Remover
Browse...
At least 10.9 MB of free disk space is required.
Simply Super Software
< Back
Next >
Cancel


Setup - T r o j a n R e m o v e r
sNipEr AlErT
الذار القناص
Select St
Where
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
Trojan Remover
Browse...
Simply Super Software
< Back
Next >
Cancel


Setup - T r o j a n R e m o v e r
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing T r o j a n R e m o v e r, then click Next.
Create a desktop icon
Create a Quick Launch ico
sNipEr AlErT
الذار القناص
Simply Super Software
< Back
Next >
Cancel


Setup - Trojan Remover
sNipEr AlErT
انذار القناص
Ready to Install
Setup is now ready
your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\Trojan Remover
Start Menu folder:
Trojan Remover
Additional tasks:
Create a desktop icon
Create a Quick Launch icon
Simply Super Software
< Back
Install
Cancel

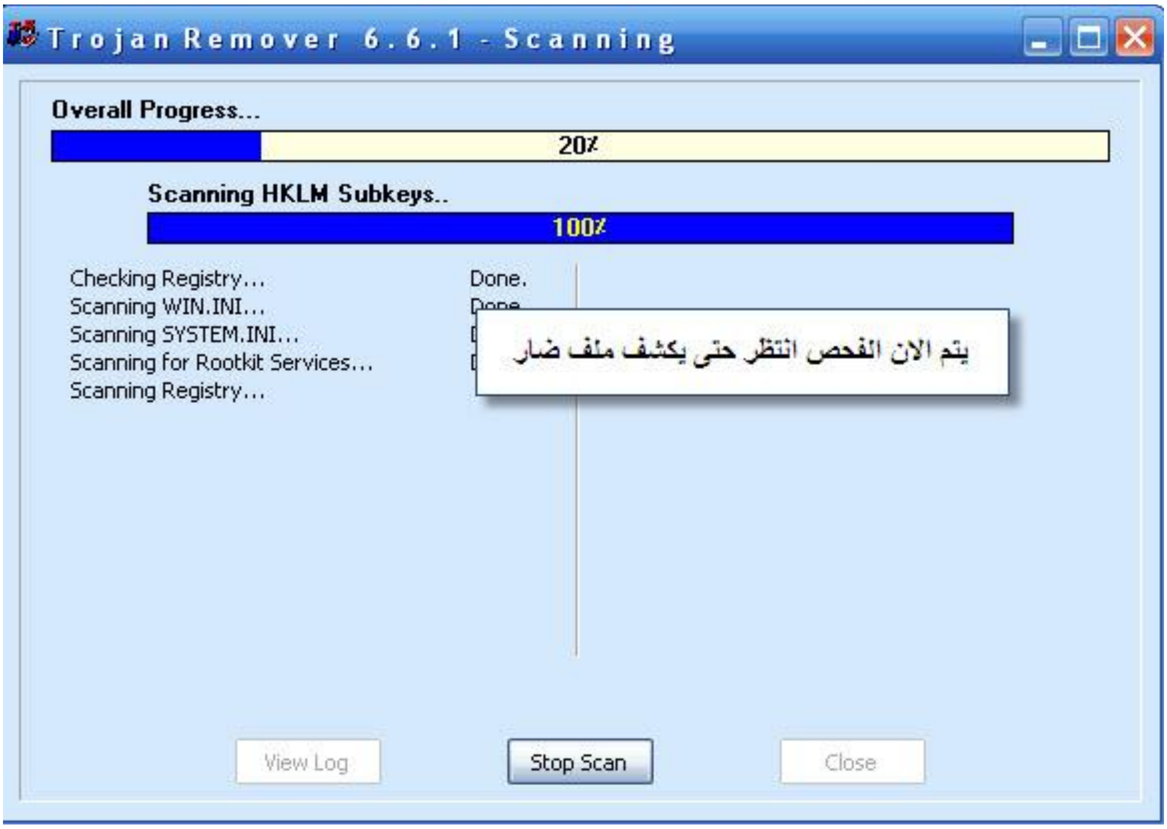

Setup - Trojan Re
sNipEr AlErT
انذار القناص
Installing
Please wait while Setup i
ter.
Extracting files...
C:\Program Files\Trojan Remover\rmt.dta
يبدأ الان التنصيب انتظر
Simply Super Software
Cancel



الان تابع معي طريقة عمل البرنامج \ انا وضعته بدون الكراك لان لن تستفيد من البرنامج لاحقا تااابع معي :




Trojan Remover 6.6.1
File Options Utilities Register Help
sNipEr AlErT
انذار القناص
Update
اضغط هنا لعميلة البدء
بالفحص الشامل
ctor & Remover
Database 6813 - 16 June 2007
Scan
Close


Trojan Remover 6.6.1 - Scanning
Overall Progress...
20%
Scanning HKLM Subkeys..
100%
Checking Registry... Done.
Scanning WIN.INI...
Scanning SYSTEM.INI...
Scanning for Rootkit Services...
Scanning Registry...
يتم الان الفحص انتظر حتى يكشف ملف ضار
View Log
Stop Scan
Close



انتظر حتى ينتهي الفحص واقفل البرنامج واعد تشغيل الجهاز وقم بتنصيب برنامج الحمايه

طيب هناك برنامج جميل جدا وظيفته حذف ملفات الاوترون التي بداخل وصلات التخزين وهو جميل جدا

ومن ميزاته عند ادخل اي وصلة تخزين يشتغل تلقائ البرنامج ليخبرك بوجود اي ملف ضار داخل الوصله

تاااابع الصور

بعد تنصيب البرنامج ادخل التسجيل الخاص به وتجده مرفق مع البرنامج

طيب لنفرض اننا شغلنا فلاش او وصلت ذاكرة فـ أول ما نشغلها تلقائي
البرنامج يشتغل ويظهر ان وجد اي ملف اوترون

تاالبع الصورة



سهل البرنامج ما يحتاج اي شرح طبعا ان ما وجد شي خلاص سليم
الفلاش بس لا تنسى افحص الفلاش بالكامل قبل تشغيله

[لتحميل البرنامج اضغط هنا]

واخيرا معلومات تهمك

****

* عدم تخزين ملفات مهمه مثل الباسوردات او صور خاصه لك بجهازك

* عدم حفظ معلومات الدخول الخاصه بالمسن او موقع لك بجهازك

* اي ملف يتم تنزيله من الانترنت يتم فحصه مباشره في مواقع الفحص

* التحديث المستمر لبرنامجك الحمايه

* عدم فتح ملف مرفق برسالة قبل تأكد من مصدره

* قبل تشغيل اي قرص خارجي او وصلة او ميموري فلاش عليك اولا فحصها قبل الدخول اليها

* هناك فيروسات تنتج ملف اوترون فعند دخولك لقرص ما .. يتم تشغيل الفيروس تلقائي

* احرص على ان الكاميرا التي لديك مغطاه بشي سميك

* تذكر ان اي ملف تجسسي قابل لتشفير لكن الاحتياط واجب فانتظر التحديثات الخاصه ببرنامج الحمايه

* تاكد من ان جدار الحمايه الي بجهاز شغال

* فحص الجهاز بالكامل ببرنامج الحماية وافضلهم برنامج الافيرا او الكاسبر 2009

****

انتهى

ارجوا اني وفقت بتوصيل اليكم المعلومه بالكامل

فتذكر انه لا يوجد جهاز بهذا العالم محمي 100٪

لكن اتبع التعليمات الموجوده بالكتاب ولا تستصعب شي

اخوكم انذار القناص

لنشر هذا الكتاب يرجى ذكر كاتبه

اعداد وتصميم

سنايبر أليرت = انذار القناص

المملكة العربية السعودية

sniper_alert@hotmail.com

Ri3@windowslive.com
